

## 明 細 書

リモートアクセスシステム、ゲートウェイ、クライアント機器、プログラム及び記憶媒体

### 参照による取り込み

- [0001] 本出願は、2004年1月21日に出願された日本特許出願第2004-012594号、2004年4月13日に出願された日本特許出願第2004-117437号の優先権を主張し、その内容を参照することにより本出願に取り込む。

### 技術分野

- [0002] 本発明は、サーバをネットワークを介して安全に遠隔操作することを可能にするセキュアリモートアクセスシステムに関する。特にクライアントを適切にサーバに接続する為の耐タンパデバイスとクライアントもしくは耐タンパデバイス上に記録するプログラム、及びリモートアクセスシステムを動作させるためのネットワーク接続技術に関する。

### 背景技術

- [0003] 近年パーソナルコンピュータ(PC)やネットワーク機器の低価格化が進み、従業員の大半にPCのような業務利用する端末を配布し、業務を行わせるようにしている企業が多数を占めるようになってきている。PCが低価格化し、利用が増えると、企業内の機器管理者のメンテナンス作業を行う必要のあるPCの数も比例して増える。このメンテナンス作業とは、例えばオペレーティングシステム(OS)や業務アプリケーションのバージョンアップやバグフィックス、ハードウェア的な障害への対応、ウィルス対策やウィルス駆除などが挙げられる。このようなメンテナンス作業を行う管理コストは非常に大きく、従業員数が増加すると、比例して莫大なものになる。
- [0004] この管理コストを低減するための一手法として、サーバクライアント方式と呼ばれるシステム運用の方式が取られている。これは、主なプログラムやデータをサーバ側に蓄積し、例えばThin Client(シンクライアント)のようなクライアント側に蓄積するデータを低減させたものである。
- [0005] サーバクライアント方式では、演算処理やデータの蓄積は主にサーバ側で行われるため、シンクライアントのようなクライアント側にて個々にOSや業務に利用するアプリケーションのバージョンアップやバグフィックス、ウィルス対策やウィルス駆除などを

行う必要性や頻度が減少するため、全体の管理コストを低減できる。

[0006] また、近年、ICチップと呼ばれるプロセッサをカード内に内蔵したICカード(別名スマートカード)が、電子認証機能をもつキーデバイスとして注目されている。ICカードとは、主に内部のICカードモジュールに中央演算処理装置(CPU)を内蔵しているカードのことを指す。ICカードのメモリにはROM、EEPROMなどが使用される。ICカードは、カード自身に演算機能を持つため、ホストからの読み書き指示の際、正しいユーザからアクセスが行われたものかどうか自身で判断する機能を持つ。また、CPU自体の偽造が困難であるため、耐タンパデバイスであるICカードモジュール(ICカードチップ)の発する情報の改ざんや、不正にICカードモジュール内部にアクセスすることが難しい。このため、高いセキュリティレベルを持つシステムを構築可能である。多くのICカードは、ユーザの登録した個人認証番号(PINコード)とカード内部に保持されたPINコードを照合するなどして、ICカード内の情報を適切にリーダライタ、もしくはホスト出力するか、もしくはしないか等の制御を行うことが可能である。ICカードは内部にEEPROMやRAMなどの書き換え可能なメモリを持ち、ユーザやカード発行者のアプリケーションや情報を格納することができる。ICカードは、外部から入力される情報に対し、その該当するカード内にしか存在し得ない情報(秘密鍵等)を用いた演算をするなどして、カード外部にカード所有者のみしか知りえない情報もしくは作りえない情報などを出力することでカード所有者を認証させたり、否認防止のための情報を出力したりすることが可能である。

[0007] また、フラッシュメモリカードは、不揮発性のメモリモジュールを内蔵したメモリカードでユーザの情報をメモリカード内に記憶することが可能である。フラッシュメモリカードの多くは「第3者からの攻撃に対するハードウェア的な耐久性」(耐タンパ性)を持っていない。耐タンパ性を持たないフラッシュメモリカードは、盗難、紛失時にカードが分解され、カード内のメモリもしくはコントローラを解析されることにより保持している情報が第3者に漏洩する可能性が少なくない。

[0008] また、特許文献1に記載されるようにフラッシュメモリインターフェースとICカード機能を持つフラッシュメモリカードが開示されている。このフラッシュメモリインターフェースとICカード機能を持つフラッシュメモリカードは、その記憶容量の大きさから、パソコ

ンやワークステーションに構築されたユーザの保管文書や設定ファイル等をカード内に保存して持ち歩くために都合がよい。

### 発明の開示

- [0009] 前述したサーバクライアント方式では、サーバとクライアントの間の認証やデータのやり取りはネットワークを介して行われる。このため、ネットワーク上の一つのクライアントから、サーバへのアクセスを行う際に、サーバ側ではアクセスしてきたクライアントが正しいクライアントであるか否か、またクライアントを利用している利用者が正しい利用者であるか否か等の検証作業を行う必要がある。また、クライアント側でも、アクセスしているサーバが正しいサーバであるか否かを検証せずには自分が欲する業務を行うことができない。もし上記のような検証を行わないとサーバ側に蓄積したデータや、利用者の持つ情報が第3者に漏洩する可能性がある。そこで、ネットワーク上での認証や、業務遂行中の送信情報などの暗号化などのセキュリティを十分に高める必要がある。
- [0010] 本発明の目的は、ICカードに実装されるICチップのような認定された耐タンパデバイスの中に利用者の認証情報を格納し、かつ、大容量のファイルを安全に格納し、持ち歩くことができるフラッシュメモリカードのようなストレージデバイスを認証デバイスとするサーバクライアントシステムによりユーザの利便性を向上させることにある。
- [0011] また、そのサーバクライアントシステムに使用可能な認証用ストレージデバイスを提供することも本発明の目的である。
- [0012] 本発明の前記並びにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。
- [0013] 本願において開示される発明のうち代表的なものの概要を説明すれば、下記の通りである。すなわち、上記の目的を達成するために本発明に係るリモートアクセスシステムは、耐タンパデバイスとストレージとコントローラの機能を実装したストレージデバイスと、前記ストレージデバイスを接続するためのリーダライタと、前記リーダライタと接続するクライアントと、ネットワークを介し前記クライアントから遠隔操作されるサーバとネットワーク上の暗号通信を行うためのゲートウェイを具備し、前記ストレージの中に、前記サーバを遠隔操作するアプリケーションと、前記ネットワーク上の通信を暗号化

する暗号化アプリケーションを記録しており、前記ゲートウェイと前記クライアントの暗号通信を行うための認証情報を前記耐タンパデバイス内に格納していることを特徴とする。

- [0014] 本発明によれば、認定された耐タンパデバイス搭載したストレージデバイスを利用者に配布し、利用者がストレージデバイスを不特定のクライアントに接続し、ストレージデバイス内の認証情報とアプリケーションを用いてサーバを遠隔操作するサーバクライアントシステムを提供することにより、利用者の使い勝手を向上することが可能で、結果としてシームレスに職場内外での業務遂行機能を利用でき、かつ操作したクライアント内に残る機密情報を低減することにより、ユーザのクライアント利用時のセキュリティ及び利便性を向上させるリモートアクセスシステムを提供できる。

#### 発明を実施するための最良の形態

- [0015] 本発明の実施の形態について、添付図面を参照しながら以下詳細に説明する。なお、図面中にて同一の参照番号を付したものは、同一の機能を有する構成要素を示し、説明の便宜上、その詳細な説明は省略する。

- [0016] (実施例1)

図1から図7を用いて、本発明に係るセキュアリモートアクセスシステムの第1の実施形態を説明する。

- [0017] 図1は、本発明の第1の実施形態を示すリモートアクセスシステムを示す図である。

- [0018] 利用者の使用するサーバ1000と複数のクライアント(クライアント1001及びクライアント1002)は、ネットワークケーブル1003、1004及び1005を介し、ネットワーク1006に接続されている。ネットワークケーブル1003、1004及び1005とネットワーク1006は、図示しないネットワークハブやスイッチにて適切に接続され、ネットワークケーブル1003、1004、1005及びネットワーク1006上の接続された機器へのパケットのルーティングが適切に行われ、正常に通信が可能な状態にある。サーバ1000は、図示しないディスプレイインターフェースを通してディスプレイ1007と接続されている。クライアント1001及び1002も同様に図示しないディスプレイインターフェースを介してそれぞれディスプレイ1008及び1009と接続されている。クライアント1001及び1002にはそれぞれユーザインターフェース1010及び1011が接続されている。ユーザイ

ンターフェース1010及び1011はキーボードやマウス、トラックボール、タッチパネル、タッチパッド、指紋リーダ、生体情報読取装置などにより構成される、クライアント1001及び1002の利用者の入力情報をそれぞれクライアント1001及び1002に送信する機能を持つ。

- [0019] リーダライタ1012及び1013はそれぞれクライアント1001及び1002に接続されており、ストレージデバイス1014を挿入する機能を持つ。ストレージデバイス1014内の後述する端子2000はリーダライタ1012の図示しない端子と接続され、クライアント1001と通信を行うことができる。ストレージデバイス1014は利用者が携帯し持ち歩くことが可能で、クライアント1001以外の例えばクライアント1002のような機器においても利用が可能な設計となっている。
- [0020] ストレージデバイス1014は、内部にコントローラ1015、耐タンパデバイス1016、ストレージ1017を実装している。コントローラ1015、耐タンパデバイス1016、ストレージ1017はそれぞれ別の集積回路として実装されているように記載されているが、機能をまとめた1つの集積回路として実装しても良い。耐タンパデバイス1016は例えばICカードチップなどのセキュリティ評価団体の定めた基準により認定を受けるかもしくは受けることが可能な水準の耐タンパ性を持つデバイスである。
- [0021] サーバ1000内部には、CPU1030、メモリ1031、ストレージ1032が実装されている。クライアント1001には、CPU3000、メモリ3001、ストレージ3002、クライアント1002には、CPU1050、メモリ1051、ストレージ1052が実装されている。
- [0022] CPU1030上にて実行される情報は、通常ディスプレイ1007により表示されるが、サーバクライアント型の処理を要求する接続がクライアント1001よりサーバ1000に行われ、認証が確立し、サーバ1000とクライアント1001の遠隔操作の暗号通信が確立した場合、クライアント1001を介してサーバ1000上でプログラムを実行した処理結果はディスプレイ1008に表示される。この際、ディスプレイ1008上に表示される情報は、ディスプレイ1007に表示される情報と表示方法を同一にしてあり、ユーザは、クライアント1001とユーザインターフェース1010を利用しているのと、サーバ1000を直接操作しているのと同様に感じ取るため、利用者のユーザビリティを高めることができる。

- [0023] 図2にストレージデバイス1014の詳細を示したブロック構成図を示す。ストレージデバイス1014は、端子2000、コントローラ1015、耐タンパデバイス1016、ストレージ1017を実装しており、それぞれが図示するように接続されている。コントローラ1015は内部にCPU2001、メモリ2002、不揮発メモリ2003、インターフェース(I/F)2004、2005、2006を持つ。ストレージ1017は、フラッシュメモリ、ハードディスク、EEPROM、MRAM、MO、光ディスク等の不揮発性の記憶媒体である。本実施例においては、ストレージ1017がフラッシュメモリであるという前提において説明を行うが、他の種類の記憶媒体であっても良い。
- [0024] コントローラ1015内のCPU2001は、不揮発メモリ2003からメモリ2002にロードされたアプリケーションを実行し、ストレージ1017のファイル管理や耐タンパデバイス1016のリセットや制御等の、耐タンパデバイス1016及び端子2000及びストレージ1017の間の通信の管理をI/F2004〜2006を介して行う。
- [0025] 不揮発メモリ2003は、公開鍵演算プログラム2050、共通鍵演算プログラム2051及びストレージ1017内のファイル管理プログラム2052を含む。また、不揮発メモリ2003は、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等を行う機能を持っている。
- [0026] 耐タンパデバイス1016は、内部にCPU2030、メモリ2031及びストレージ2032を含む。コプロセッサ2033はCPU2030の演算機能のうち暗号機能などの補完するコプロセッサであるが、CPU2030の計算速度が高速である場合、実装しなくてもよい。CPU2030は、ストレージ2032からメモリ2031にロードされたアプリケーションを実行し、後述する共通鍵による暗復号、非対称鍵による暗復号、ストレージ2032内のファイル管理、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等を行う機能を持つ。耐タンパデバイス1016は、電圧変動などの様々な攻撃に対して強い耐性のある、セキュリティ評価団体の定めた基準により認定を受けるかもしくは受けることが可能な水準の耐タンパ性を持つデバイスである。
- [0027] ストレージ2032は、EEPROM、MRAM、フラッシュメモリなどの不揮発性ストレージである。ストレージ2032は、内部に秘密鍵2040、PIN情報2041、ログ情報2042、証明書2043、公開鍵2044、PIN検証プログラム2045、鍵証明書格納プログラム

2046、公開鍵演算プログラム2047、共通鍵演算プログラム2048、鍵生成プログラム2049等を保存する。保存されたプログラムは、1つでも複数でも良い。ストレージ2032内のデータやプログラムは、メモリ2031にロードされ、CPU2030を動作させたり、コントローラ1015を経由して耐タンパデバイス1016外部に送信される。

[0028] 秘密鍵2040は、利用者の認証や通信路を暗号化するためなどの鍵であり、1つでも複数個でも良い。秘密鍵2040は、対応する鍵アルゴリズムの種類によって異なるフォーマットにて記述される。秘密鍵2040内の一つの秘密鍵に対応する公開鍵の集まりが公開鍵2044であり、対応する証明書の集まりが証明書2043である。証明書2043は、秘密鍵2040に対応する公開鍵2044の証明書であり、サーバ1000や外部の認証局より発行されたものである。また、証明書2043は公開鍵2044の証明書とそのほかの証明書を発行した証明期間のルート認証局や中間認証局の証明書などその他の認証情報を含む。証明書2043のフォーマットは例えば国際電気通信連合(ITU)の定めるX. 509の仕様を満たすものである。証明書2040内に格納される情報は、公開鍵と公開鍵に対する署名の他に、例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名や電子メールアドレスなどの利用者の情報及び拡張領域といった項目によって構成される。証明書2010はカード内からクライアント1001及び1002、サーバ1000内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

[0029] PIN情報2041は、耐タンパデバイス1016外部から耐タンパデバイス1016内部の情報を出力させたり、演算を行わせたりする利用者の権利を検証するための情報である。PIN情報2041は、暗証番号(PINコード)でも良いし、パスフレーズと呼ばれるような桁数の長い文字列でも良いし、指紋、虹彩、顔形、声紋、静脈などによる生体認証の根拠となる生体認証情報でも良い。

[0030] ログ情報2042は、耐タンパデバイス1016の利用履歴が記録されたもので、CPU3000もしくは2001もしくは2030が動作するたびに追記されたり、耐タンパデバイス1016の外部から適切な権利を持つ利用者が追記したり、読み出したりする。ログ情報2042は、第三者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

- [0031] PIN検証プログラム2045は、PIN情報2041が耐タンパデバイス1016外部から検証用に入力されたPIN情報と合致するか検証するプログラムである。検証結果が正しいければ、耐タンパデバイス1016は利用者が内部の情報や演算資源を利用可能な状態にする。PIN検証プログラム2045は、ストレージ2032内にあり、メモリ2031にロードされるプログラムやストレージ2032上に保存される情報ごとに利用権限を定め、個別に認証を行う。例えば、耐タンパデバイスが通電された後の利用時に一度PIN検証プログラムにて正しいと判断された利用者には以降のアクセスにてPIN検証を求めなかったり、利用のたびにPIN検証を行ったりできるよう設定することができる。
- [0032] 鍵証明書格納プログラム2046は、ストレージ2032内に保存されている秘密鍵2040や公開鍵2044や証明書2043を耐タンパストレージ1016外部へ出力したり、耐タンパストレージ1016外部から内部へ取り込んでストレージ2032内に格納したりする機能を持つ。鍵証明書格納プログラム2046を利用するためにはPIN検証プログラム2045による検証が終了する必要がある。ただし、証明書2043や公開鍵2044を出力するだけであるなら、PIN検証プログラム2045による検証が不要としても良い。鍵証明書格納プログラム2046は、外部へ鍵や証明書を入出力する際に外部のCPU3000もしくは2001もしくは2030とセッション鍵を交換し安全な暗号化通信路を設けて鍵や証明書をやり取りする機能を持っている。
- [0033] 公開鍵演算プログラム2047及び共通鍵演算プログラム2048は、それぞれ前述の公開鍵演算プログラム2050及び共通鍵演算プログラム2051と同様の機能を持つ。鍵生成プログラム2049は、秘密鍵2040及び公開鍵2044のうちの1つの鍵のペアや対象鍵の秘密鍵(共通鍵)を生成する機能を持つ。作成された公開鍵や共通鍵はストレージ2032内に保存されたり、外部に出力される。非対称鍵の秘密鍵は、秘密鍵2040内に保存される。
- [0034] ストレージ1017は内部に利用者を識別するための証明書2010、利用者がストレージデバイス1014を利用して操作を行ったログ情報2011、デバイスアクセス用ライブラリ2012、デバイス管理用ツール2013、デバイスドライバ2014、インターフェースハンドラ2015、インストーラ2016、遠隔操作端末用アプリケーション2017、暗号化通信路構築用アプリケーション2018、業務アプリケーション2019、一時記憶領域20



20、認証情報のコピー2021を記録している。

- [0035] 証明書2010は、クライアント1001やサーバ1000が利用者やストレージデバイス1014を識別する演算を行うために利用する。証明書2010のフォーマットは例えばITUの定めるX. 509の仕様を満たすものなどであればよい。証明書2010内には例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名、電子メールアドレスやストレージデバイス固有の識別番号等の利用者やストレージデバイスの情報、拡張領域といったものが記録されている。証明書2010はストレージデバイス1014内やクライアント1001、サーバ1000内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。
- [0036] ログ情報2011は、利用者がストレージデバイス1014を利用して操作を行った際に、CPU2001もしくはCPU2030もしくはクライアント1001もしくはサーバ1000の指示により更新される。ログ情報2011は、サーバ1000上のアプリケーションやクライアント1001上のアプリケーションより利用されるか、利用者が自分の利用状況を確認するために利用される。ログ情報2011は、第3者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。
- [0037] デバイスアクセス用ライブラリ2012は、クライアント1001にて動作する複数のアプリケーションがストレージ1017にアクセスする際に利用する、ファイル管理、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等の機能を利用するための関数群である。通常、後述するインストーラ2016によって、クライアント1001にインストールされて利用するが、直接、デバイスアクセス用ライブラリ2012がクライアント1001上のアプリケーションから利用されても良い。
- [0038] デバイス管理用ツール2013は、ストレージデバイス1014を管理するためのツールであり、例えば、利用者の認証番号を変更するツールや閉塞したストレージデバイスを初期化するツールやストレージデバイス上のプログラムやファームウェア、鍵情報、証明書の書き換えツールや、ストレージデバイス1014をデバッグする際に必要となるデバッグ用のモニタリングツールや、ストレージデバイスのマニュアルやヘルプファイルや、遠隔地からサーバの電源を投入するWake up on LANのような機能などを利

用しクライアント1001やサーバ1000をリモートから電源投入や電源遮断をする電源管理するツールを含む。デバイス管理用ツール2013は、後述するインストーラ2015によりクライアント1001にインストールされても良いし、利用者がクライアント1001へ直接ロードして利用しても良い。

- [0039] デバイスドライバ2014は、ストレージデバイス1014の動作に必要な情報をOSに提供したり、動作を管理するプログラムであり、後述するインストーラ1015によりクライアント1001にインストールされる。
- [0040] インターフェースハンドラ2015は、デバイスドライバ2014を管理するミドルウェアで、クライアント1001やサーバ1000上で動作するアプリケーションとデバイスドライバ2014を接続させる役割を果たす。
- [0041] インストーラ2016は、ストレージ1017上に存在するアプリケーションや情報、ドライバなどをクライアント1001やサーバ1000にインストールする際に利用者が利用する。インストーラ2016によってインストールされるアプリケーションや情報、ドライバ等は、インストール終了後に削除されても良いが、利用者が別の機器に接続してストレージデバイス1014を利用する際のためにストレージデバイス上に保存しておく。
- [0042] 遠隔操作端末用アプリケーション2017は、クライアント1001からサーバ1000を遠隔操作するために利用する。遠隔操作端末用アプリケーション2017は、ターミナルサービスやリモートデスクトップ等といったクライアント1001やサーバ1000のOSの持つ標準のサービスやアプリケーションでもよい。遠隔操作端末用アプリケーション2017は、インストーラ2016によってクライアント1001にインストールされて利用されるか、もしくはストレージデバイス1014からクライアント1001に直接ロードされて利用される。
- [0043] 暗号化通信路構築用アプリケーション2018は、クライアント1001とサーバ1000との間の通信を暗号化させるために利用される。暗号化通信路構築用アプリケーション2018は、サーバ1000とクライアント1001の間で秘密鍵を共有させ、その秘密鍵を用いることによりサーバ1000とクライアント1001の間に暗号化通信路を成立させる。この秘密鍵の共有に耐タンパデバイス1016内の秘密鍵等の秘密情報を用いてもよいし、秘密鍵を共有するプロセス内に耐タンパデバイス1016内の秘密情報を用い

た認証を用いても良い。

[0044] 業務アプリケーション2019は、利用者がクライアント1001を利用する際に利用するアプリケーションである。業務アプリケーション2019は、例えばサーバ上のウェブベースのアプリケーションを利用するのであれば、ウェブブラウザであり、データベースを利用するのであれば、データベース操作クライアントである。ストレージ1017上の全ての情報が、耐タンパデバイス1016内にある秘密鍵2040のうちのいくつかの秘密鍵かサーバ1000もしくはクライアント1001上に保持する秘密鍵のうちのいくつかによって暗号化されていてもよいし、平文で記録されていてもよい。前者であれば、利用者に提供するセキュリティが向上する。また、コントローラ1015や耐タンパデバイス1016内において利用者認証が済んでいないとストレージ1017にアクセスできないようになっている場合、利用者に提供するセキュリティが向上する。

[0045] 一時記憶領域2020は、業務アプリケーション2019等のアプリケーションをクライアント1001上で実行するときに、アプリケーションの作成する一時ファイルを保存しておく領域である。業務アプリケーション2019やサーバ1000もしくはクライアント1001上の業務遂行用アプリケーションは、ビットマップのキャッシュなどの一時記憶ファイルを一時記憶領域2020内に作成する。一時記憶領域が暗号化されていない場合、利用者が利用を停止する際には、コントローラ1015もしくはクライアント1001上のOSもしくはアプリケーションの指示により一時記憶ファイルは消去される。このことにより、利用者の作成する一時ファイルはストレージデバイス上に記憶され、クライアント1001内の情報が第三者によって危険にさらされても利用者の利用した情報は安全に保護され、電源を切断したクライアント1001からの利用者の機密情報やプライバシーを含んだ情報はより漏洩しにくくなる。

[0046] 図12にストレージ1017上に記録された業務アプリケーション2019やクライアント1001などにインストールされたアプリケーションから一時記憶領域2020を利用する際の処理方法をフローチャートにて示した図を示す。図12のフローチャートに示される処理は、アプリケーションの実行されるCPU1030、もしくは3000において行われる。例えば、遠隔操作端末用アプリケーション2017や業務アプリケーション2019は、CPU3000上にて実行され、サーバ1000上のアプリケーションは、CPU1030上で

実行されることになる。この際、利用者が利用するアプリケーションが起動される(1200)と、一時記憶領域2020がアプリケーションに定義されているかどうかと利用可能かどうか調べられる(12001)。処理12001において未定義もしくは利用不可能の場合一時記憶領域2020の領域の定義と利用可能化(12002)が行われる。次に、一時記憶領域の容量が十分かなど利用可能かどうかのチェックが行われる(12004)。容量不足等の問題が検出された場合は容量不足など問題解決処理が行われ(12005)異常状態から復帰できれば(12006)処理が継続されるが、出来ない場合は、アプリケーションは異常終了する(12007)。次にアプリケーションの処理が開始される(12003)、一時記憶領域2020への入出力が行われる(12008)。アプリケーションの処理が継続されるようであれば、処理12004へ戻る。アプリケーションが終了される場合、一時記憶領域2020への入出力12010が行われる。処理12010はアプリケーションの利用した情報の消去とその確認作業である。処理12010により利用者の利用した情報が適切に保全されたり、多くの場合は諸居されることにより、利用者の持つプライバシーを含む情報や秘匿情報が保護される。異常が無ければ、アプリケーションは終了する(12011)。

- [0047] アプリケーションによって、一時記憶領域2020の定義方法がいくつか存在する。一つの方法は、アプリケーションが起動される際に、利用者ごとにクライアント1001上に設けられた利用者のプロフィールに記載されてある一時記憶領域の設定をアプリケーションが読み込むことにより、一時記憶領域2020の場所をアプリケーションが特定するやり方である。この際、利用者のプロフィールは、OSもしくはアプリケーションによって定義される利用者の設定情報で、ストレージ3002もしくは、ストレージ1017に記録されている。もう一つの方法は、アプリケーションが起動される際に、利用者に対し、OSもしくはアプリケーションがダイアログなどの確認手段をディスプレイ1008上に表示するなどして、利用者に入力を促し、アプリケーションが一時記憶領域の設定を特定することである。この確認手段は多くはアプリケーションの最初の起動時に行われるが、毎起動時に行われても良い。以上のいずれかの方法によりアプリケーションは利用者の利用環境に対応した一時記憶領域の設定を行う。一度利用者が定義した情報は、クライアント上のストレージ3002もしくはストレージ1017上に情報を記録

することにより、アプリケーション起動時にアプリケーションが再度利用すればよい。

- [0048] 認証情報のコピー2021は、耐タンパデバイス1016内にある例えば、証明書2043や公開鍵2044のような認証情報のコピーである。この認証情報のコピー2021は、耐タンパデバイス1016内にある公開鍵2044や証明書2043やPIN情報2041等のコピーである。
- [0049] 図3に認証情報のコピー2021の例を示す。証明書1(5001)〜証明書N(5003)は証明書2043の一部である。ミドルウェアの認証情報5004は、サーバ1000もしくは、クライアント1001のミドルウェアが認証情報のコピーが改ざんされていないかを検査するハッシュ値と署名やミドルウェアのバージョン情報、認証情報のコピーの作成された時刻情報などのミドルウェアの認証情報が含まれる。
- [0050] 一般的に耐タンパデバイス1016、コントローラ1015間の通信速度はストレージ1017、コントローラ1015間の通信速度より遅いことが多い。このため、クライアント1001上のOSもしくはアプリケーションが耐タンパデバイス1016内の認証情報をストレージ1017にキャッシュもしくはコピーしておくことにより、利用者がストレージデバイスを利用する際に証明書2043の読み出しに要する時刻を短縮することができ、ユーザビリティを向上させることができる。認証情報のコピー2021は、ストレージデバイス1014が利用されるたびに検証されることが望ましく、その際に、認証情報のコピー2021の中の、ハッシュ値や耐タンパデバイス1016内の秘密鍵による署名や、クライアント1001上のOSもしくはアプリケーションによる署名が利用される。
- [0051] 図4にクライアント1001の詳細を示したブロック構成図を示す。クライアント1001は、内部にCPU3000、メモリ3001、ストレージ3002、インターフェース(I/F)3020、3021、3022、3023を持つ。ストレージ3002は、フラッシュメモリ、ハードディスク、EEPROM、MRAM、MO、光ディスク等の不揮発性の記憶媒体である。
- [0052] CPU3000は、ストレージ3002からメモリ3001にロードされたアプリケーションを実行し、ディスプレイ1008、ネットワーク1006、ユーザインターフェース1010、リーダライタ1012との通信をそれぞれ、I/F3020、3021、3022、3023を介して行う。
- [0053] ストレージ3002は、証明書3010、ログ情報3011、デバイスアクセス用ライブラリ3012、デバイス管理用ツール3013、デバイスドライバ3014、インターフェースハンドラ

3015、遠隔操作端末用アプリケーション3016、暗号化通信路構築用アプリケーション3017、業務アプリケーション3018が保存される。

[0054] 証明書3010は、クライアント1001やサーバ1000が利用者やストレージデバイス1014を識別する演算を行うために利用する。証明書3010のフォーマットは例えばITUの定めるX. 509の仕様を満たすものなどであればよい。

[0055] 証明書3010内には例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名、電子メールアドレスやストレージデバイス固有の識別番号等の利用者やストレージデバイスの情報、拡張領域といったものが記録されている。証明書3010はストレージデバイス1014内の証明書2043やストレージ1017内の証明書2010のコピーや独自に利用者が登録した利用者や証明書を証明するルート認証局や中間認証局やストレージデバイス1014などの耐タンパデバイスの証明書であり、クライアント1001、サーバ1000内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

[0056] ログ情報3011は、利用者がクライアント1001の操作を行った場合に、CPU3000もしくはサーバ1000の指示により更新される。ログ情報3011は、サーバ1000上のアプリケーションやクライアント1001上のアプリケーションより利用されるか、利用者が自分の利用状況を確認するために利用される。ログ情報3011は、第3者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

[0057] 図5に利用者がクライアント1001にストレージデバイス1014を挿入し、サーバ1000を利用する際の利用者、ストレージデバイス1014、クライアント1001、サーバ1000間にて行われる通信の詳細を示した図を示す。利用者はクライアント1001の利用を開始するまでに利用者の認証情報やクライアント1001を動作させるためのアプリケーションが保存されたストレージデバイス1014をクライアント1001のリーダライタに接続する。利用者が、クライアント1001を利用したことがない場合は、利用者はストレージデバイス1014内のインストーラ2016を利用し、デバイスドライバ2014やデバイス管理ツール2013や遠隔端末用アプリケーション2017のようなサーバ1000を操作するために必要な情報もしくはアプリケーションをクライアント1001にインストールす

る。この際、クライアント1001によってストレージデバイス1014から直接実行できるアプリケーションのインストールを行う必要はない。

- [0058] 利用者は、まずシーケンス4000に示すようにクライアント1001に動作確認要求を行う。クライアント1001はサーバ1000にサーバ動作確認を行う(4001)利用者はサーバ1000の動作を確認できなかった場合は、ストレージデバイス1014上のもしくはインストーラ2016にてクライアント1001上に用意された遠隔地からサーバの電源を投入するローカルエリアネットワーク(LAN)を利用して機器の電源投入を行うようなWake up on LANのような機能を利用してサーバ1000の電源投入を行う。この場合、サーバ1000の、ネットワークに対するI/Fのみは常時通電されており、IDとパスワードのセットやネットワークボードのMACアドレス等、何らかの認証情報を利用してサーバ1000の起動が行われる(4002、4003)。この操作によりサーバ1000は起動される(4004)。サーバの起動が完了した際、利用者はクライアント1001にログイン要求を入力する(4005)。クライアント1001内に遠隔操作アプリケーション2017及び暗号化通信路構築用アプリケーション2018がインストールされていない場合、この時点にてクライアント1001にロードされる(4006)。次にクライアント1001からサーバ1000にログイン要求が行われる(4007)。サーバ1000のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者の認証において公開鍵インフラストラクチャ(PKI)を用いた認証が必要もしくは可能である場合、サーバ1000からの認証情報の要求(4008)、クライアント1001からの証明書の要求(4009)、ストレージデバイス1014からの証明書の送信(4010)、クライアント1001からの署名の要求(4011)が行われる。ストレージデバイス1014において署名を行う場合、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。

- [0059] 本実施例では、暗証番号を利用した例を示す。ストレージデバイス1014からの暗証番号要求(4012)が行われた後、クライアント1001から利用者へ暗証番号要求表示4013がディスプレイ1008などを利用して行われる。利用者が暗証番号をユーザインターフェース1010とクライアント1001を介してストレージデバイス1014に送信す

ると(4014、4015)、ストレージデバイス1014内のCPU2001もしくはCPU2030においてサーバ1000、クライアント1001から送信された情報に対し、秘密鍵2040のうちの一つもしくはいくつかを用いた電子署名が作成される(4016)。作成された署名は、クライアントに送信される(4017)。クライアント1001は、証明書2010、2043などの認証情報と作成された署名の送信を行う(4018)。次に、サーバ1000及びクライアント1001は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う(4019)。この鍵交換4019は、遠隔操作端末用アプリケーション2017か暗号化通信路構築用アプリケーション2018により行われる。シーケンス4019において交換された秘密共有鍵を用いて、サーバ1000及びクライアント1001は暗号化通信路を構築し、2者の間で通信される情報は暗号化される。暗号化通信路が構築された段階で、ユーザは、サーバ1000または、クライアント1001、ストレージデバイス1014上に保存されているアプリケーションを起動し、業務遂行をする(4020)。

[0060] 業務遂行中は、CPU2001もしくはCPU2030もしくはサーバ1000もしくはクライアント1001は、ログ情報2011、2042、3011に情報を追記し、利用者の業務遂行を適切に監視する。記載されたログ情報は、改ざん防止の処理を施され、ストレージデバイス1014やクライアント1001内に保存されるが、利用者の利用開始時や利用終了時など適切なタイミングでサーバ1000に送信される。

[0061] 利用者の利用するサーバ1000の管理を行う管理者は、ログ情報2011、2042、3011の情報とサーバ1000に送信される情報を監査し、利用者が管理者が作成したポリシーに違反する利用を行った際に、サーバ1000もしくはクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションを行う。ポリシー違反は、例えば、ログの改ざんや、異常な利用時間、異常な通信量、ネットワーク1006を介した異常なアクセス、クライアント1001内に存在する異常なファイルの検出、ファイルやアプリケーションのアップデートの不備などが該当する。サーバ1000もしくはクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションとは、サーバ1000及びクライアント1001への利用者のログインの禁止や電源遮断、ストレージデバイス1014の閉塞などが該当する。ストレージデバイス1014



の閉塞とは、PIN検証プログラム2045の利用する情報を変更し、利用者がストレージデバイス1014を利用できないようにすることである。

- [0062] 利用者の業務など、サーバ1000の利用が終了した場合、利用者は、クライアント1001に対しサーバ遮断要求を行う(4021)。サーバ遮断要求はクライアント1001からサーバ1000に送信される(4022)。サーバ1000及びクライアント1001はセッションの遮断4023を行う。サーバ1000は、利用者の利用情報のログをサーバ1000上に記憶し(4024)、サーバ1000のサーバ電源遮断を行う。利用者がサーバ遮断要求4021を行わなければ、サーバ電源遮断4025は行われず。サーバ電源遮断後は、また図5に示すシーケンスで業務遂行が行われる。
- [0063] 図6は、利用者がサーバ1000及びクライアント1001及びストレージデバイス1014を利用するために管理者が行うストレージデバイス1014の初期化操作を説明した図である。図6にて説明される一連の動作は、図5に示した利用者の利用が開始される前もしくは利用者がカードを閉塞もしくは紛失し、利用権限を失った際に行われる。
- [0064] クライアント6000は、クライアント1001と同様にディスプレイやユーザインターフェースやリーダライタを接続されたクライアントで、管理者がストレージデバイス1014の書き込みを行うために利用する。
- [0065] まず、管理者は、利用者の氏名ユーザ番号、電子メールアドレスやストレージデバイス固有の識別番号等をクライアント6000を通じ、サーバ1000に登録することにより、サーバ1000より利用者の認証情報を作成する。利用者の認証情報及び証明書の作成と書き込み要求を行う(6001)。ここで、ストレージデバイス1014は、既にストレージデバイス供給者から鍵証明書格納プログラム2046などの各種プログラムが書き込まれている。また、利用者の公開鍵証明書は、ストレージデバイス1014もしくはクライアント6000もしくは管理者が別途生成した秘密鍵に対応する公開鍵を6001にて送付することにより得られる。作成された認証情報と公開鍵証明書は、クライアント6000を経由してストレージデバイスへ書き込まれる(6002)。次に管理者は、ストレージデバイス1014内の認証情報と鍵の利用権をコントロールするための情報を変更する(6003、6004)。この操作によってストレージデバイス1014は、署名要求や鍵書き換え要求、鍵のエクスポートインポート要求に対する利用権を変更される。利用権の

変更は、情報に対するアクセスキーの変更や、暗証番号の変更である。変更されたアクセスキーや暗証番号は、管理者が保管したり、他の耐タンパデバイスに格納したり、利用者に通知する。

[0066] 次に、管理者は、アプリケーションの書き込み要求を行い、クライアント6000は、アプリケーションの書き込みを行う。ここで言うアプリケーションとは、デバイスアクセス用ライブラリ2012、デバイス管理用ツール2013、デバイスドライバ2014、インターフェースハンドラ2015、インストーラ2016、遠隔操作端末用アプリケーション2017、暗号化通信路構築用アプリケーション2018、業務アプリケーション2019などである。

[0067] 次に、管理者は、サーバ接続試験要求(6007)を行い、サーバ接続試験が行われる(6008)。サーバ接続試験6008は、図5にて示した利用者が行うサーバへの接続や業務遂行のプロセスを管理者が行い、ストレージデバイス1014内に記録された情報やアプリケーションの有効性を確認するものである。接続と業務遂行プロセスが正しく行われた場合、ストレージデバイス1014は、利用者に送付される。この際、ストレージデバイス1014は利用者のIDや顔写真や氏名などを印刷されるか、シール針付けするなどされる。また、ストレージデバイス1014を管理するための情報に対するアクセスキーや暗証番号もストレージデバイス1014を送付するのとは別の封書などの方法で利用者に送付される。

[0068] 図11は、本実施例のクライアント1001上で動作するミドルウェアについて説明した図である。クライアント1001上で動作する遠隔操作端末用アプリケーション2017や暗号化通信路構築用アプリケーション2018、業務アプリケーション2019のようなアプリケーション11000は、図示するように2つの経路を利用してリーダライタ1012及びストレージデバイス1014にアクセスを行う。カード内のファイルアクセスやファイル管理を行いたい場合は、ファイルアクセス用API11001、ファイルアクセス用ドライバ11002、リーダライタ1012内のリーダライタファームウェア11003を経由し、ストレージデバイス1014内のカードOS及びアプリケーション11004が呼び出される。また、カード内の耐タンパデバイス2032に命令を発するなど、セキュリティ認証にかかわる命令を実行したい場合は、インターフェースハンドラ3015、デバイス3014、リーダライタ1012内のリーダライタファームウェア11003を経由し、ストレージデバイス1014

内のカードOS及びアプリケーション11004が呼び出される。この際、ファイルアクセス用ドライバ11002、リーダライタファームウェア11003、デバイス3014は、お互いの命令が同時に発生することが無いように常にストレージデバイス1014とリーダライタ1012のアクセス状態を監視し、ストレージデバイス1014に対して適切なアクセスがなされるように、自身で命令のストックや拒否などの輻輳制御を行う。

[0069] 図13は、デバイスドライバ3014とファイルアクセス用ドライバ11002の行う輻輳制御をフローチャートを用いて説明した図である。ドライバ3014及び11002は、OSの起動時などに初期化され、処理が開始される(13000)。ファイルアクセス用ドライバ11002への要求もしくは待機した要求があるかどうかチェックが行われ(13001)、要求があった場合、リーダライタを介したカードへのファイルアクセスが行われる(13002)。次に、デバイスドライバ3014への要求があるかどうかのチェックが行われる(13003)。ある場合は、リーダライタを介したCPU2030へのアクセスが行われる(13004)。ファイルアクセス用ドライバ11002への要求がこの時点であるかどうかチェックが行われ(13005)、要求があった場合、ファイルアクセス用ドライバ11002への要求待機処理が行われる。この要求待機処理は、ファイルアクセス用ドライバ11002において行われ、要求待機用に作られたメモリ領域に、待機すべき要求がストックされる。ストックされた要求は、次に処理13002が実行される際に処理される。ただし、処理13002により処理が行われるまでのストックしている時間があらかじめ定めた一定量を超えた場合は、処理13005内で、アプリケーションへタイムアウトなど異常を通知し、処理を破棄する。デバイスドライバ3014への要求が終了したと認識できるかどうかチェックが行われ(13007)処理が完了しない場合は、処理13004から再処理が行われる。

[0070] また、OSからの終了要求がチェックされ(13008)、要求が無い場合は、再び処理13001から処理が開始される。上記のようなデバイスドライバ3014及びファイルアクセス用ドライバ11002による輻輳制御により、リーダライタを介したストレージデバイス1014のアクセスは、一般的なストレージデバイスと同様に保たれる。輻輳制御とは、ファイルアクセスに関する命令と、耐タンパデバイスに対する命令との輻輳を制御することで、ファイルアクセス用ドライバ11002は、一般的なマスタストレージデバイスドラ

イバでも、マストレージデバイスドライバに接続するアッパーフィルタドライバやローワーフィルタドライバで行ってもよい。また、リーダーライタファームウェアに命令を退避させるメモリ領域もしくはバッファを設けて命令を待機させ、輻輳を制御してもよい。

[0071] さらに、輻輳制御について詳細に説明する。輻輳制御とは、下記に示すような待機処理もしくは競合解決処理を示す。ここで、輻輳を制御するのは、後述する待機させられたコマンドリストをクライアント上のメモリ領域に作成しソフトウェア的に処理しても良いし、リーダーライタのファームウェアにてソフトウェア的に解決しても良いし、リーダーライタ上にバッファを設けてハードウェア的に解決しても良い。

[0072] 図14は、デバイスドライバ3014とファイルアクセス用ドライバ11002における輻輳制御により発せられるコマンドの様子を示すタイムチャートである。CPU2030へのアクセスのためのコマンド1、コマンド2が順にドライバより発せられるようアプリケーションから指示があったとする。図14のファイルアクセス用コマンドに示すようにコマンド1がストレージデバイス1014に発せられ、そのレスポンス1の応答がある。次にコマンド2がストレージデバイス1014に発せられ、そのレスポンス2の応答がある。このコマンドの発行、応答の間にファイルアクセス用コマンド3やコマンド4が発せられたとする。この際、ファイルアクセス用ドライバはコマンド3やコマンド4を待機させられたコマンドリストに格納する。図13における処理13002においてCPU2030へのアクセスのためのコマンドからの入力が無いと判断される場合、待機させられたファイルアクセス用コマンド3が発せられ、そのレスポンス3の応答がある。次に待機させられたファイルアクセス用コマンド4が発せられ、そのレスポンス4の応答がある。全体として、ストレージデバイス1014に送受信されるコマンドとレスポンスは、例えば、図14における「全てのコマンドとレスポンス」に示すように、順にコマンド1、レスポンス1、コマンド2、レスポンス2、コマンド3、レスポンス3、コマンド4、レスポンス4のようになる。

[0073] 上記のように、本実施形態に示したクライアント1001は、耐タンパストレージ機能を搭載したストレージデバイス1014を挿入しサーバ1000を遠隔操作する事により、利用者に安全で、使い勝手良く利用できる業務システムを構成することが可能となる。

[0074] また、利用者は、利用するクライアント1001からクライアント1002に変更したとしても、クライアント1001を利用するのと同様の操作感覚にて業務遂行を行うことができ

るため、利用者の使い勝手が向上する。

- [0075] また、利用者が利用を停止する際には、利用者が利用していた一時記憶ファイルが消去されるため、クライアント1001内の情報が第3者によって危険にさらされても利用者の利用した情報は安全に保護され、電源を切断したクライアント1001からの利用者の利用した機密情報やプライバシーを含んだ情報はより漏洩しにくくなることにより、利用者の利便性を向上させる。
- [0076] また、本実施の形態では、クライアント1001及びサーバ1000を別の構成として記載したが、逆にクライアント1001がサーバ1000の機能を兼ねたり、サーバ1000をクライアント1001の代わりに使用したりすることが可能でもよい。また、サーバ1000、クライアント1001、1002は、PCやPersonal Digital Assistants (PDA)、ワークステーションであるように記載したが、高機能複写機、現金自動支払機(ATM)、携帯電話、デジタルスチルカメラ、ビデオカメラ、音楽再生(録音)装置、販売時点商品管理システム、街角端末、Intelligent Transport Systems (ITS)用送信機、券売機、決済端末、改札機、自動販売機、入退室管理装置、ゲーム機、公衆電話、注文取り用携帯端末、電子財布、有料放送受信機、医療カード管理装置等として同様である。
- [0077] (実施例2)
- 図7から図9用いて、本発明に係るセキュアリモートアクセスシステムの第2の実施形態を説明する。
- [0078] 図7は、本発明の第2の実施形態のリモートアクセスシステムを示す図である。
- [0079] 利用者の使用するサーバ1000とクライアント1001、ストレージデバイス1014は、第1の実施形態にて説明したものと同様である。ゲートウェイ7000は、クライアント1001とサーバ1000の通信の暗号化と利用者、利用機器認証を行う中継機器である。
- [0080] ゲートウェイ7000は、一般的にファイヤーウォール、暗号化ゲートウェイ、バーチャルプライベートネットワーク(VPN)ゲートウェイなどと呼ばれる。本実施例では、ゲートウェイ7000は、ファイヤーウォールと暗号通信機能をインストールされたサーバ機であるとして説明を行うが、例えば、ネットワークルータや無線LANアクセスポイント、ネットワークハブ、ブロードバンドルータなどでも良い。ネットワーク7001は、例えばイン

ターネットや地域IPネットワークのような、公衆回線であり、ネットワーク1006より通信内容の盗聴や改ざんの危険性の高いネットワークである。クライアント1001は、ネットワーク7001越しにサーバ1000を遠隔操作するため、ゲートウェイ7000とクライアント1001の間にて暗号通信と暗号通信を行うための認証を行う。

[0081] ゲートウェイ7000は、CPU7002、メモリ7003、ストレージ7004を持ち、動作時にストレージ7004内に設定された暗号通信及び認証用アプリケーションがメモリ7003にロードされCPU7002にて通信の制御を行う。ゲートウェイ7000は、認証用サーバ7005に直接もしくはネットワークを経由して接続している。認証用サーバ7005は、ゲートウェイ7000にて暗号通信を行う際の認証情報を蓄積し、ゲートウェイ7000の問合せに対して応答したり、接続されたリーダライタ7007を介して、ストレージデバイス1014の初期化や活性化、個人化などを行う。認証用サーバ7005は、内部認証局を持っていても良いし、外部の認証局の証明書リストや証明書リボケーションリストを管理し、ゲートウェイ7000に通知する役割だけを持っていても良い。

[0082] 図8に、本実施形態のリモートアクセスシステムを利用する際のストレージデバイス1014の初期化と利用者がクライアント1001にストレージデバイス1014を挿入し、サーバ1000を利用する際の管理者、利用者、ストレージデバイス1014、クライアント1001、ゲートウェイ7000、サーバ1000間にて行われる通信の詳細を示した図を示す。

[0083] 管理者は、ストレージデバイス1014を認証サーバ7005と通信が可能なリーダライタ7007に挿入する。管理者は、利用者の氏名ユーザ番号、電子メールアドレスやストレージデバイス固有の識別番号等をクライアント1001を通じ、認証サーバ7005に登録することにより、認証サーバ7005より利用者の認証情報を作成する。利用者の認証情報及び証明書の作成と書き込み要求を行う(8001)。ここで、ストレージデバイス1014は、既にストレージデバイス供給者から鍵証明書格納プログラム2046などの各種プログラムが書き込まれている。また、利用者の公開鍵証明書は、ストレージデバイス1014もしくは認証サーバ7005もしくは管理者が別途生成した秘密鍵に対応する公開鍵を8001にて送付することにより得られる。作成された認証情報と公開鍵証明書は、ストレージデバイス1014へ書き込まれる。次に管理者は、ストレージデ

バイス1014内の認証情報と鍵の利用権をコントロールするための情報を変更する(8003、8004)。この操作によってストレージデバイス1014は、署名要求や鍵書き換え要求、鍵のエクスポートインポート要求に対する利用権を変更される。利用権の変更は、情報に対するアクセスキーの変更や、暗証番号の変更である。変更されたアクセスキーや暗証番号は、管理者が保管したり、他の耐タンパデバイスに格納したり、利用者に通知する。

[0084] 次に、管理者は、アプリケーションの書き込み要求を行い、認証サーバ7005は、アプリケーションの書き込みを行う。ここで言うアプリケーションとは、デバイスアクセス用ライブラリ2012、デバイス管理用ツール2013、デバイスドライバ2014、インターフェースハンドラ2015、インストーラ2016、遠隔操作端末用アプリケーション2017、暗号化通信路構築用アプリケーション2018、業務アプリケーション2019などである。

[0085] 次に、管理者は、サーバ接続試験要求(8007)を行い、サーバ接続試験が行われる(8008)。サーバ接続試験8007は、ストレージデバイス1014内に記録された情報やアプリケーションの有効性を確認するものである。接続と業務遂行プロセスが正しく行われた場合、ストレージデバイス1014は、利用者に送付される(8009)。この際、ストレージデバイス1014を管理するための情報に対するアクセスキーや暗証番号もストレージデバイス1014を送付するのとは別の封書などの方法で利用者に送付される。

[0086] 次に、利用者はクライアント1001の利用を開始するまでに利用者の認証情報やクライアント1001を動作させるためのアプリケーションが保存されたストレージデバイス1014をクライアント1001のリーダライタに接続する。利用者が、クライアント1001を利用したことがない場合は、利用者はストレージデバイス1014内のインストーラ2016を利用し、デバイスドライバ2014やデバイス管理ツール2013や遠隔端末用アプリケーション2017のようなサーバ1000を操作するために必要な情報もしくはアプリケーションをクライアント1001にインストールする。この際、クライアント1001によってストレージデバイス1014から直接実行できるアプリケーションのインストールを行う必要はない。

[0087] 利用者は、まずシーケンス8010に示すようにクライアント1001にゲートウェイ接続

要求を行う。クライアント1001はゲートウェイ7000にサーバ動作確認を行う(8011)ゲートウェイ7000のリモート機器からのログインに対するセキュリティポリシーの設定によるが、利用者の認証をPKIを用いた認証が必要もしくは可能である場合、ゲートウェイ7000からの認証情報の要求(8012)、クライアント1001からの証明書の要求(8013)、ストレージデバイス1014からの証明書の送信(8014)、クライアント1001からの署名の要求(8015)が行われる。ストレージデバイス1014において署名を行う場合、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。本実施例では、暗証番号を利用した例を示す。ストレージデバイス1014からの暗証番号要求(8016)が行われた後、クライアント1001から利用者へ暗証番号要求表示(8017)がディスプレイ1008などを利用して行われる。利用者が暗証番号をユーザインターフェース1010とクライアント1001を介してストレージデバイス1014に送信すると(8018、8019)、ストレージデバイス1014内のCPU2001もしくはCPU2030においてサーバ1000、クライアント1001から送信された情報に対し、秘密鍵2040のうちの一つもしくはいくつかを用いた電子署名が作成される(8020)。作成された署名は、クライアントに送信される(8021)。クライアント1001は、証明書2010、2043などの認証情報と作成された署名の送信を行う(8022)。次に、サーバ1000及びクライアント1001は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う(8023)。この鍵交換8023は、暗号化通信路構築用アプリケーション2018により行われる。シーケンス8023において交換された秘密共有鍵を用いて、ゲートウェイ7000及びクライアント1001は暗号化通信路を構築し、2者の間で通信される情報は暗号化される。

- [0088] 次に、利用者は、シーケンス8030に示すようにクライアント1001に動作確認要求を行う。クライアント1001はサーバ1000にサーバ動作確認を行う(8031)利用者はサーバ1000の動作を確認できなかった場合は、ストレージデバイス1014もしくはインストーラ2016にてクライアント1001上に用意された遠隔地からサーバの電源を投入するLANを利用して機器の電源投入を行うようなWake up on LANのような機能を利用してサーバ1000の電源投入を行う。この場合、サーバ1000の、ネットワーク



に対するI/Fは常時通電されており、IDとパスワードのセットやネットワークボードのMACアドレス等、何らかの認証情報を利用してサーバ1000の起動が行われる(8032、8033)。この操作によりサーバ1000は起動される(8034)。サーバの起動が完了した際、利用者はクライアント1001にログイン要求を入力する(8035)。この操作は、クライアント1001内の遠隔操作アプリケーション2017により行われる。遠隔操作アプリケーションがインストールされていない場合、この時点にてクライアント1001にロードされる。サーバ1000のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者の認証をPKIを用いた認証が必要もしくは可能である場合、サーバ1000からの認証情報の要求などが行われ、8012〜8023と同様の署名の作成と送信がサーバ1000に対し行われる。利用者は、ゲートウェイ7000において強固な認証を通過しているので、サーバ1000がゲートウェイ7000からの通信を信頼できるとすると、ログイン要求8035を行う際のサーバ1000の認証はIDとパスワード認証などの簡便なものでも良い。

- [0089] 暗号化通信路構築とサーバ1000へのログインが完了した段階で、ユーザは、サーバ1000または、クライアント1001、ストレージデバイス1014上に保存されているアプリケーションを起動し、業務遂行をする(8036)。
- [0090] 業務遂行中は、CPU2001もしくはCPU2030もしくはサーバ1000もしくはクライアント1001は、ログ情報2011、2042、3011に情報を追記し、利用者の業務遂行を適切に監視する。記載されたログ情報は、改ざん防止の処理を施され、ストレージデバイス1014やクライアント1001内に保存されるが、利用者の利用開始時や利用終了時など適切なタイミングでサーバ1000に送信される。
- [0091] 利用者の利用するサーバ1000の管理を行う管理者は、ログ情報2011、2042、3011の情報とサーバ1000に送信される情報を監査し、利用者が管理者が作成したポリシーに違反する利用を行った際に、サーバ1000もしくはクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションを行う。ポリシー違反は、例えば、ログの改ざんや、異常な利用時間、異常な通信量、ネットワーク1006を介した異常なアクセス、クライアント1001内に存在する異常なファイルの検出、ファイルやアプリケーションのアップデートの不備などが該当する。サーバ1000もしく

はクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションとは、サーバ1000及びクライアント1001への利用者のログインの禁止や電源遮断、ストレージデバイス1014の閉塞などが該当する。ストレージデバイス1014の閉塞とは、PIN検証プログラム2045の利用する情報を変更し、利用者がストレージデバイス1014を利用できないようにすることである。利用者の業務など、サーバ1000の利用が終了した場合、利用者は、クライアント1001に対しサーバ遮断要求を行う(8037)。サーバ遮断要求はクライアント1001からサーバ1000に送信される(8038)。サーバ1000及びクライアント1001はセッションの遮断8039を行う。サーバ1000は、利用者の利用情報のログをサーバ1000上に記憶し(8040)、サーバ1000のサーバ電源遮断を行う。利用者がサーバ遮断要求8037を行わなければ、サーバ電源遮断8041は行われない。サーバ電源遮断後は、また8010以降のシーケンスで業務遂行が行われる。

[0092] 図9に、本実施形態のリモートアクセスシステムのネットワーク構成を示したブロック図を示す。図中9000にて示されたネットワークとネットワークに接続した機器のグループは、利用者が中心的に利用するネットワークと機器のグループである。ネットワークと機器のグループ9000は、例えば、利用者が常に勤務するオフィスのローカルエリアネットワーク(LAN)とLANに接続された機器である。9000内には、ユーザの利用可能なサーバ1000、クライアント1002、部門サーバ9001、PC9002、ゲートウェイ9006、7000、認証サーバ7005がLAN9003を中心に接続されている。また、9010にて示されたネットワークとネットワークに接続した機器のグループは、利用者が出張時などに利用する所属外の事業部などのWAN上のネットワークと機器のグループである。9010内には、ユーザの利用可能なクライアント9008、ゲートウェイ9007がネットワーク9005を中心として接続されている。また、ネットワーク7001のような社外のネットワークにルータ9004を介してクライアント1001が接続されている。

[0093] ここで、利用者は、ストレージデバイス1014を持ち歩くことにより、LAN上のクライアント1002、WAN上のクライアント9008、インターネットを介しLAN9003に接続しているクライアント1001を利用して、LAN9003と接続されたサーバ1000、部門サーバ9001、PC9002を利用することができる。この際、LAN上のクライアント1002、W

AN上のクライアント9008からLAN9003と接続されたサーバ1000、部門サーバ9001、PC9002を利用する際は、ゲートウェイ9007、9006では、通信の暗復号を行わず、ゲートウェイ7000を利用する場合、通信の暗復号を行うようにすれば、利用者の利用手順の簡略化を図りつつ、通信内容の秘匿が可能である。ここで、部門サーバ9001とは、LAN上に設置されたウェブサーバやメールサーバやリモートログインして演算を行うターミナルサーバなどを示す。PC9002は、利用者の所属する部門が共有などで利用している共有リソース管理用PCや出張者用貸し出しPCなどを示す。

[0094] 上記のように、本実施形態に示したクライアント1001は、耐タンパストレージ機能を搭載したストレージデバイス1014を挿入しサーバ1000、部門サーバ9001、PC9002などを遠隔操作することにより、利用者に安全で、使い勝手良く利用できる業務システムを構成することが可能となる。

[0095] また、利用者は、利用するクライアント1001からクライアント1002、9008に変更したとしても、様々な異なる業務執行場所において、クライアント1001を利用するのと同様の操作感覚にて業務遂行を行うことができるため、利用者の使い勝手が向上する。また、サーバ1000、クライアント1001、1002、9008は、PCやPDA、ワークステーションであるように記載したが、高機能複写機、ATM、携帯電話、デジタルスチルカメラ、ビデオカメラ、音楽再生(録音)装置、販売時点商品管理システム、街角端末、ITS用送信機、券売機、決済端末、改札機、自動販売機、入退室管理装置、ゲーム機、公衆電話、注文取り用携帯端末、電子財布、有料放送受信機、医療カード管理装置等として同様である。

[0096] (実施例3)

図10を用いて、本発明に係るセキュアリモートアクセスシステムの第3の実施形態を説明する。

[0097] 図10は、本発明の第3の実施形態を示すリモートアクセスシステムを示す図である。

[0098] 利用者の使用するサーバ10000は、サーバ1000と同等の機能をもつ複数個のサーバ(PC)の集合体である。サーバ10000はサーバ10032、10042、…、10052上

にある、それぞれCPU10030、10040、…、10050、メモリ10031、10041、…、10051により動作する。図10では、利用者は、サーバ10032を利用し、CPU10030上にて実行された情報をディスプレイ1008に出力させて業務を遂行している。サーバ10000は、切り替え器10004を利用してサーバ10032、10042、…、10052と接続するユーザインターフェース10003及びディスプレイ10002を選別している。また、サーバ10000は、制御装置10001に接続されている。制御装置10001は、ネットワーク1005に接続しており、サーバ10000と同様にストレージデバイス1014を持つ適切な利用者が利用可能である。ここで、利用者がサーバ10032、10042、…、10052のいずれかを利用しようとした際に、制御装置10001は、サーバ10032、10042、…、10052の電源管理、電源のオンオフ、状態のクライアントへの通知を行う。特に、クライアント1001からのサーバ10032、10042、…、10052への通信が不通になった際は、利用者は、制御装置10001にログインし、サーバ10032、10042、…、10052の状態を確認したり、電源をオンオフしたりする。制御装置10001内にはハードディスクやフラッシュメモリなどのサーバブート用のストレージが実装しており、このストレージ上のデータを用いてサーバ10032～10052がブートアップする。このことにより、利用者のサーバ管理の工数が減少する。

[0099] 上記のように、本実施形態に示したサーバ10000及び制御装置10001を、耐タンパストレージ機能を搭載したストレージデバイス1014を挿入したクライアント1001より利用することにより、サーバ10000は、1つの筐体の内部に複数の類似した機能を持つサーバを持つ特長から、管理者のサーバ10032、10042、…、10052の管理工数を削減することができる。また、利用者が制御装置10001を利用することによりサーバの電源管理などが容易に行えるため、利用者の使い勝手が向上する。

[0100] (実施例4)

図1、図15、図16を用いて、本発明に係るセキュアリモートアクセスシステムの第4の実施例を説明する。本実施形態は、セキュアリモートアクセスシステムを利用する利用者が、多くの人間が使用するような公衆のクライアント機器を介して業務を遂行する場合に有効である。

一般に、公衆のクライアント機器には、ある個人あるいは複数の利用者が使用する

ためのアプリケーションや個人的な設定情報などが保存されている。本実施形態では、それらアプリケーションや個人設定情報をクライアント機器1001内部のストレージ3002にインストールや格納をしないようなセキュアリモートアクセスシステムを提示する。さらに、利用者の操作量を軽減することによって利便性の高いセキュアリモートアクセスシステムを提示する。

[0101] 図15は、本発明の第4の実施例におけるストレージデバイス1014の詳細を示したブロック構成図である。本実施例では、第1の実施例におけるストレージデバイス1014内部のストレージ1017の中に、新たにブートプログラム15001とOSプログラム15002を追加する。ブートプログラム15001は、クライアント1001が起動される際に、そのBIOS (Basic Input/Output System) によって最初に実行されるプログラムであり、クライアント1001用のOSを起動させる役割を持つ。OSプログラム15002は、前記ブートプログラム15001によってストレージデバイス1014からクライアント1001内部のメモリ3001上に読み込まれ起動されるクライアント1001用のOSのプログラムである。

[0102] 利用者の使用するサーバ1000とクライアント1001、1002は、第1の実施例にて説明したものと同様である。

[0103] 図16は、利用者がクライアント1001に図15に示したストレージデバイス1014を挿入し、サーバ1000を利用する際の利用者、ストレージデバイス1014、クライアント1001、サーバ1000間にて行われる通信の詳細を示した図である。利用者はクライアント1001を起動するまでに利用者の認証情報やクライアント1001を動作させるためのブートプログラム、OSプログラム、アプリケーション等が保存されたストレージデバイス1014をクライアント1001のリーダライタ1012に接続しておく必要がある。また、クライアント1001のBIOSは、リーダライタ1012を通してブートプログラムを検出するのが、ストレージ3002を通して検出するのに優先するようにあらかじめ設定されている必要がある。第1の実施例との違いは、利用者がクライアント1001を利用したことがない場合でも、利用者はデバイスドライバ2014やデバイス管理ツール2013や遠隔端末用アプリケーション2017のようなサーバ1000を操作するために必要な情報もしくはアプリケーションをクライアント1001のストレージ3002にインストールする必要がない

ことである。

[0104] 利用者は、まずシーケンス16001に示すようにクライアント1001の電源を投入する。それによってクライアント1001のBIOSが起動し(16002)、ストレージデバイス1014にブートプログラム15001を要求する(16003)。ストレージデバイス1014は、これに応じてブートプログラム15001を送信する(16004)。クライアント1001のBIOSはブートプログラム15001を実行してブート処理を開始する(16005)。ブート処理の中では、ブートプログラム15001によって、ストレージデバイス1014にOSプログラム15002を要求する(16006)。ストレージデバイス1014は、これに応じてOSプログラム15002を送信する(16007)。OSプログラム15002は、クライアント1001内部のメモリ3001上に読み込まれ、起動される(16008)。これ以降、ストレージデバイス1014に格納されているアプリケーション、ライブラリ、ドライバ、管理ツール等(2012〜2019)は、このOS上に読み込まれて動作することが可能となる。OSプログラム15002にはOS起動直後自動的に特定のアプリケーションを実行するように記述されている。これに従い、クライアント1001は遠隔操作アプリケーション2017及び暗号化通信路構築用アプリケーション2018、さらにその実行に必要なライブラリ、ドライバ等をストレージデバイス1014に要求する(16009)。ストレージデバイス1014は、これに応じてそれらのアプリケーションを送信する(16010)。そして、クライアント1001はそれらのアプリケーションを起動する(16011)。

[0105] それらのアプリケーションのプログラムには、利用者が接続したいサーバのIPアドレスがあらかじめ記述されている。クライアント1001は自動的にそのIPアドレスのサーバ1000に動作確認を行う(16012)。クライアント1001はサーバ1000の動作を確認できなかった場合は、Wake on LANのような機能を利用してサーバ1000の電源投入を行う。この場合、サーバ1000の、ネットワークに対するI/Fのみは常時通電されており、IDとパスワードのセットやネットワークボードのMACアドレス等、何らかの認証情報を利用してサーバ1000の起動が要求される(16013)。これによりサーバ1000は起動される(16014)。サーバの起動が完了した際、クライアント1001から自動的にサーバ1001にログイン要求が行われる(16015)。サーバ1000のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者

の認証において公開鍵インフラストラクチャ(PKI)を用いた認証が必要もしくは可能である場合、サーバ1000からクライアント1001に認証情報を要求し(16016)、クライアント1001からストレージデバイス1014に証明書を要求し(16017)、ストレージデバイス1014からクライアント1001に証明書を送信し(16018)、クライアント1001からストレージデバイス1014に署名を要求する(16019)。

[0106] ストレージデバイス1014において署名を行う場合、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。本実施例では、暗証番号を利用した例を示す。ストレージデバイス1014からの暗証番号要求(16020)が行われた後、クライアント1001から利用者へ暗証番号要求表示16021がディスプレイ1008などを利用して行われる。利用者が暗証番号をユーザインターフェース1010とクライアント1001を介してストレージデバイス1014に送信すると(16022、16023)、ストレージデバイス1014内のCPU2001もしくはCPU2030においてサーバ1000、クライアント1001から送信された情報に対し、秘密鍵2040のうちの一つもしくはいくつかを用いた電子署名が作成される(16024)。作成された署名は、クライアントに送信される(16025)。クライアント1001は、証明書2010、2043などの認証情報と作成された署名の送信を行う(16026)。

[0107] 次に、サーバ1000及びクライアント1001は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う(16027)。この鍵交換16027は、遠隔操作端末用アプリケーション2017か暗号化通信路構築用アプリケーション2018により行われる。シーケンス16027において交換された秘密共有鍵を用いて、サーバ1000及びクライアント1001は暗号化通信路を構築し、2者の間で通信される情報は暗号化される。暗号化通信路が構築された段階で、利用者は、サーバ1000、クライアント内のメモリ3001、またはストレージデバイス1014上に格納されているアプリケーションを起動し、業務遂行をする(16028)。

[0108] 業務終了後、クライアント1001は図5のシーケンス4021〜4025のようにサーバ1000との通信を遮断し、利用者はクライアント1001の電源を切断してストレージデバイス1014をリーダライタ1012から抜き取る。これによって、メモリ3001上の情報も揮発

するため、クライアント1001内部には利用者が使用したアプリケーションや個人情報などが一切残らない。これにより、公衆のクライアントを使用したセキュアリモートアクセスシステムにおいて、利用者のプライバシーが保護される。

[0109] また、クライアント1001上で動作するOSプログラムは利用者自身がストレージデバイス1014内に管理しているので、クライアントにインストールされているOSに第3者がひそかに設置したコンピュータウイルス等の不正プログラムにより利用者の暗証番号が盗聴されるなどの危険も回避される。これにより、公衆のクライアントを使用したセキュアリモートアクセスシステムにおいて、利用者のセキュリティも保護される。

[0110] また、図16のように、利用者がクライアント1001の利用を開始してから業務対象サーバ1000に接続するまでの間の過程は、ブートプログラム15001とOSプログラム15002によって自動化されているので、利用者の操作は電源投入16001と暗証番号送信16022のみである。これにより、利用者にとってのセキュアリモートアクセスシステムの利便性が向上する。

[0111] (実施例5)

第5の実施例は、第4の実施例におけるセキュアリモートアクセスシステムを利用する利用者が、安全であると信用できるクライアントを介して業務を遂行する場合に有効である。

[0112] 第4の実施例におけるセキュアリモートアクセスシステムでは、クライアント1001で動作するOSをストレージデバイス1014から読み出している。しかし、利用者が公衆クライアント機器のように安全性が保証されないクライアント機器ではなく、自身の所有するPCやレンタルオフィスや出張先の管理されたオフィスのPCのように安全であると信用できるクライアントを使用する場合には、OSをストレージデバイス1014から読み出さずに、クライアント内にインストールされているOSを利用してもよい。

[0113] そのため、本実施例のリーダライタ1012は起動モードを選択する機能を有する。具体的には、図17Aのように機械的なスイッチを搭載している。このスイッチは、第4の実施例におけるブートプログラム15001をストレージデバイス1014からクライアント1001に送信可能にしたり、不可能にしたりを切り替えることができる。このスイッチでブートプログラム15001を送信可能にすれば、セキュアリモートアクセスシステムは図1



6のように(つまり、第4の実施例のように)動作する。

- [0114] 一方、ブートプログラム15001を送信不可能にすれば、OSプログラム15002ではなくクライアント内にインストールされているOSが起動するため、セキュアリモートアクセスシステムは図5のように(つまり、第1の実施例のように)動作する。図17Aはその処理を示した図である。利用者は、スイッチ17000でブートプログラム15001を送信するか送信しないかを選択する。ブートプログラムを送信しないことを選択した場合、ストレージデバイス1014からは、クライアント機器へダミーデータ17001が送信される。ダミーデータ17001がクライアント1001のメモリ3001上にロードされると、BIOSはストレージデバイス1014を通してのOS起動に失敗するため、その代わりにストレージ3002内のOSを起動する。
- [0115] なお、該スイッチ等の切替手段を用いて、記憶媒体側(リーダライタ1012も含む)からOSプログラム15002の送信可否を選択してもよい。但し、この場合、ブートプログラムは記憶媒体側からクライアント機器へ送られている。該切替手段を操作し、OSプログラムを送らない設定とした場合、記憶媒体側からクライアント機器へはダミーデータが送信される。ダミーデータを受信したブートプログラムは、ブートプログラムに予め設定されたOSプログラムの読み込み先の機器からOSプログラムを読み出すこととなる。この場合、OSプログラムの読み込み先の機器としては、クライアント1001内のストレージ3002でも、ネットワーク上の計算機上のストレージでも良い。
- [0116] また、図17A、Bにおいて記憶媒体側からのブートプログラムの送信が拒否された場合であって、かつ、クライアント機器側のブートプログラムをロードした場合も、上記と同様に、該ブートプログラムの内容によって、自機器あるいは他の機器の記憶装置からOSプログラムを読み出すことが可能である。
- [0117] このような起動モードを選択するための機械的なスイッチは、ストレージデバイス1014に搭載してもよい。一般に、PC用のディスクデバイスにおいて、ブートプログラムが格納されている領域は最初の論理セクタアドレスで示される領域である。このスイッチでその領域のデータの読み出しを許可するか否かを切り替えることによって、ブートプログラム15001の送信を制御できる。結果として、このスイッチで起動モードを選択することができる。図17Bはその処理を示した図である。スイッチ17002でブートプ

ログラム15001を送信するかダミーデータ17003を送信するかを選択する。ダミーデータ17003がクライアント1001のメモリ3001上にロードされると、BIOSはストレージデバイス1014を通してのOS起動に失敗するため、その代わりにストレージ3002内のOSを起動する。

- [0118] 起動モードを選択するもう1つの方式としては、ブートプログラム15001がクライアント1001を構成する様々なデバイスを調査することによって、それが安全な端末であると信用できるか否かを判別する方法である。図17Cはその処理を示した図である。メモリ3001上にロードされたブートプログラム15001がクライアント1001を信用できないものと判断したならば、OSプログラム15002をメモリ3001上にロードして起動する。信用できるものと判断したならば、ストレージ3002内のOSを起動する。なお、クライアント1001内のデバイスを調査する際に、ストレージデバイス1014内の耐タンパデバイス1016を利用してデバイス認証処理を実行すれば、より信頼性の確証が得られる。この場合、あらかじめ耐タンパデバイス1016内のストレージ2032内にデバイス認証処理プログラムやデバイス認証処理に必要な鍵や証明書などを格納しておき、ブートプログラム15001からの指示によってストレージデバイス1014内のCPU2030がデバイス認証処理を実施するのが好ましい。ブートプログラム15001がクライアント1001を構成する様々なデバイスを調査する方法は、例えば、ブートプログラム15001がクライアント1001内にあるかクライアント1001に接続されているCPUやメモリ、ストレージデバイス、ネットワークカードなどに割り当てられた製造番号やMACアドレスのように番号と部品に1対1につけられた番号や証明書を調査や検証することである。この番号や証明書は各CPUやメモリ、ストレージデバイス、ネットワークカードの製造者やクライアントや部品の製造者や管理者などが番号付けを行う。

- [0119] 図17Cにおいて起動モードを選択するもう1つの方法としては、ストレージ3002内のOSが暗号化やパスワードロックがかかった状態であるかどうかを調査してから、OSプログラム15002をメモリ3001上にロードして起動するようにしても良い。この場合、上記したデバイス認証は記憶媒体側のCPU2030が行い、ストレージ3002内のOSが暗号化やパスワードロックがかかった状態であるかどうかの調査はクライアント機器側のCPU3000が行うこととなる。

[0120] 図18は、図17Cを用いて説明した第5の実施例のOSの起動を行う際の動作を説明するためのフローチャートである。

ブートプログラムの起動後(18000)、上述した方法により、クライアント1001に記憶媒体からロードされたブートプログラム15001が、デバイス認証に必要な情報を集めてCPU2030に送信して、該CPU2030でデバイス認証が成功したかどうか判定される(18001)。

判定結果が認証成功(YES)であった場合、ストレージ3002がパスワードロックなどのロック機能や暗号化機能によってパスワード等の情報の入力無しには内部に格納されているOSなどのデータを読み取ることができないようになっているかどうか判定される(18002)。

[0121] 次にストレージデバイス1014から認証情報が取得できるかが判定される(18003)。18003での判定が失敗した場合(NO)、利用者からロックや暗号化を解除する情報の入力を促すよう画面表示し、入力をCPU3000およびストレージ3002に送信する(18004)。18003の判定に成功(YES)した場合もしくは、18004の動作を終了した場合、ストレージ3002は受け取った情報を用いて、例えばパスワードの比較など、内部に格納されている情報に受け取った情報が適合しているかどうか検査を行う(18005)。受け取った情報が検査に合格すれば(YES)、利用者はストレージ3002の正当な利用権を持つことが証明されるので、ストレージ3002内部に格納されているOSプログラム15002やその他のデータが利用可能になる。よって、ストレージデバイス3002を用いてOSの起動が行われ(18006)、OSの起動は終了する(18007)。18002の判定が失敗(NO)だった場合は、ロックや暗号化がされていないということであるため、ストレージデバイス3002を用いてOSの起動が行われ(18006)、OSの起動は終了する(18007)。18005の判定に失敗した(NO)場合、もしくは、18001の判定に失敗した場合(NO)、OSプログラム15002をメモリ3001上にロードして起動し(18008)、OSの起動は終了する(18009)。

[0122] なお、図17Cにおいて認証の判断結果に基づきOSの読込先の切り替えを行う手段は、スイッチのような機械的手段でもよいし、コントローラとバスの組み合わせのようなソフトウェア的手段でもよい。

[0123] 以上のように、実施例5に示したストレージデバイス及びリーダライタ及びクライアントを利用することにより、クライアントが信頼できるか否か、または、クライアント内のOSやストレージが利用できるか否か等を判定して適切に利用者の利用すべきブートプログラムやOSプログラムを選択することができ、利用者のクライアントを利用する際の安全性を高めることができる。また、自動的に起動すべきOSを選択したり、認証情報を入力させることにより、利用者の利便性を高めたセキュアリモートアクセスシステムを提供できる。

上記記載は実施例についてなされたが、本発明はそれに限らず、本発明の精神と添付の請求の範囲の範囲内で種々の変更および修正をすることができることは当業者に明らかである。

#### 図面の簡単な説明

[0124] [図1]本発明の第1の実施形態のセキュアリモートアクセスシステムを説明するためのブロック構成図。

[図2]本発明の第1の実施形態のストレージデバイスを説明するためのブロック構成図。

[図3]本発明の第1の実施形態の認証情報のコピーの構成を示す図。

[図4]本発明の第1の実施形態のクライアントの詳細を示したブロック構成図。

[図5]本発明の第1の実施形態の利用者、ストレージデバイス、クライアント、サーバ間にて行われる通信の詳細を示した図。

[図6]本発明の第1の実施形態の管理者が行うストレージデバイスの初期化操作を説明した図。

[図7]本発明の第2の実施形態のリモートアクセスシステムを示す図。

[図8]本発明の第2の実施形態の利用者、管理者、ストレージデバイス、クライアント、ゲートウェイ、サーバ間にて行われる通信の詳細を示した図。

[図9]本発明の第2の実施形態のリモートアクセスシステムのネットワーク構成を示したブロック図。

[図10]本発明の第3の実施形態を示すリモートアクセスシステムを示す図。

[図11]本発明の第1の実施形態のソフトウェア構成を示す図。

[図12]本発明の第1の実施形態のアプリケーションから一時記憶領域を利用する際の処理方法を示すフローチャート。

[図13]本発明の第1の実施形態のドライバにおける輻輳制御を行う際の処理方法を示すフローチャート。

[図14]本発明の第1の実施形態のドライバにおける輻輳制御を示すタイムチャート。

[図15]本発明の第4の実施形態のストレージデバイスを説明するためのブロック構成図。

[図16]本発明の第4の実施形態の利用者、ストレージデバイス、クライアント、サーバ間にて行われる通信の詳細を示した図。

[図17A]本発明の第5の実施形態のストレージデバイス、リーダライタ、クライアント間にて行われる処理を示した図。

[図17B]本発明の第5の実施形態のストレージデバイス、リーダライタ、クライアント間にて行われる処理を示した図。

[図17C]本発明の第5の実施形態のストレージデバイス、リーダライタ、クライアント間にて行われる処理を示した図。

[図18]本発明の第5の実施形態のOSの起動を行う際の動作を説明するためのフローチャート。

### 請求の範囲

- [1] リモートアクセスシステムであって、  
サーバと、  
前記サーバにアクセスするクライアント機器と、  
前記サーバと前記クライアント機器とを接続するネットワークと、  
前記クライアント機器に接続され、前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、業務アプリケーションと、耐タンパ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体とを有し、  
前記記憶媒体には、前記クライアント機器で、前記遠隔操作アプリケーション、前記暗号化アプリケーション、前記業務アプリケーションを動作させるミドルウェアが格納され、  
前記クライアント機器のCPUは、前記ミドルウェアを実行し、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとクライアント機器間で通信を行うことを特徴とするリモートアクセスシステム。
- [2] 請求項1記載のリモートアクセスシステムであって、  
前記ファイルアクセス用ドライバ、あるいは前記デバイスドライバからの命令が発生した場合、予め定めた順序で、前記命令を制御することを特徴とするリモートアクセスシステム。
- [3] 請求項2記載のリモートアクセスシステムであって、  
前記ファイルアクセス用ドライバ、あるいは前記デバイスドライバからの命令が発生した場合、前記デバイスドライバからの命令を優先して実行することを特徴とするリモートアクセスシステム。
- [4] 請求項1記載のリモートアクセスシステムであって、  
前記記憶媒体は、更に、一時記憶領域を有し、  
前記クライアント機器で実行された処理により生じたデータを、当該一時記憶領域

に格納することを特徴とするリモートアクセスシステム。

- [5] リモートアクセスシステムであって、  
サーバと、  
前記サーバに接続されたゲートウェイと、  
前記サーバにアクセスし、前記ゲートウェイとの間で認証処理を行うクライアント機器と、  
前記サーバと前記クライアント機器とを接続するネットワークと、  
前記クライアント機器に接続され、前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、業務アプリケーションと、耐タンパ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体とを有し、  
前記記憶媒体には、前記クライアント機器で前記遠隔操作アプリケーション、前記暗号化アプリケーション、前記業務アプリケーションを動作させるミドルウェアが格納され、  
前記クライアント機器のCPUは、前記ミドルウェアを実行し、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとクライアント機器間で通信を行うことを特徴とするリモートアクセスシステム。
- [6] 請求項1記載のリモートアクセスシステムであって、  
前記サーバは、複数のサーバと、当該複数のサーバに接続された制御装置を有し、  
前記クライアント機器は、前記制御装置にアクセスし、前記複数のサーバの電源管理を行うことを特徴とするリモートアクセスシステム。
- [7] 請求項1記載のリモートアクセスシステムであって、  
前記記憶媒体は、前記耐タンパ領域内に格納された認証情報のコピーを保持することを特徴とするリモートアクセスシステム。
- [8] サーバと、ネットワークを介し前記サーバにアクセスするクライアント機器と、前記クラ

クライアント機器に接続され、前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、耐タンパ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体とを有し、前記クライアント機器から前記サーバにアクセスするリモートアクセスシステムにおけるゲートウェイであって、

前記記憶媒体から前記クライアント機器にロードされるミドルウェアにより動作される、インターフェースハンドラ、デバイスドライバを介して送信される前記認証情報に基づき、前記クライアント機器を操作するユーザの認証処理を行うことを特徴とするゲートウェイ。

[9] サーバにネットワークを介し接続されるクライアント機器であって、

前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、耐タンパ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体が接続されるリーダライタを有し、

前記リーダライタを介し、前記記憶媒体からロードされるミドルウェアを実行し、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとの通信を行うことを特徴とするクライアント機器。

[10] サーバと、ネットワークを介し前記サーバにアクセスするクライアント機器との間でリモートアクセスを行うためのプログラムであって、

前記クライアント機器にインストールされ、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとクライアント機器間の通信を実現させるためのプログラム。

[11] リモートアクセスシステムであって、

サーバと、

ネットワークを介して前記サーバにアクセスするクライアント機器と、



前記クライアント機器に接続され、前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、業務アプリケーションと、耐タンパ格納領域に格納された前記サーバに対する遠隔操作のための認証情報と、前記クライアント機器が起動される際に該クライアント機器が有するBIOSによって実行されるブートプログラムと、OSプログラムとが格納された記憶媒体とを有し、

前記クライアント機器のBIOSは、前記記憶媒体に格納されたブートプログラムを前記クライアント機器が有するブートプログラムよりも先に検出するよう設定され、

前記クライアント機器は、電源を投入後に、前記記憶媒体に格納されたブートプログラムを検出して、前記ブートプログラムにより、前記記憶媒体に格納されたOSプログラムを取得して実行することを特徴とするリモートアクセスシステム。

[12] 請求項11記載のリモートアクセスシステムであって、

前記クライアント機器は表示手段を有し、

前記OSプログラムが起動されて前記遠隔操作アプリケーションが実行された後、前記サーバとの通信認証要求が前記表示手段に最初に表示されることを特徴とするリモートアクセスシステム。

[13] 請求項11記載のリモートアクセスシステムであって、

前記記憶媒体は、前記OSプログラムを前記クライアント機器上で起動するか否かを選択するための手段を有し、

前記選択するための手段で前記OSプログラムを前記クライアント機器上で起動することを選択した場合、

前記記憶媒体上のブートプログラムを前記クライアント機器に送信して前記記憶媒体上に格納されたOSプログラムを前記クライアント機器上で実行させ、

前記選択するための手段で前記OSプログラムを前記クライアント機器上で起動しないことを選択した場合、

ダミーデータを前記クライアント機器に送信して、前記クライアント機器に予め格納されたOSプログラムを前記クライアント機器上で実行させることを特徴とするリモートアクセスシステム。

- [14] 請求項11記載のリモートアクセスシステムであって、  
前記記憶媒体は、当該記憶媒体のリーダライタを介して前記クライアント機器に接続され、  
前記リーダライタは、前記OSプログラムを前記クライアント機器上で起動するか否かを選択するための手段を有し、  
前記選択するための手段で前記OSプログラムを前記クライアント機器上で起動することを選択した場合、  
前記記憶媒体上のブートプログラムを前記クライアント機器に送信して前記記憶媒体上に格納されたOSプログラムを前記クライアント機器上で実行させ、  
前記選択するための手段で前記OSプログラムを前記クライアント機器上で起動しないことを選択した場合、  
ダミーデータを前記クライアント機器に送信して、前記クライアント機器に予め格納されたOSプログラムを前記クライアント機器上で実行させることを特徴とするリモートアクセスシステム。
- [15] 請求項13記載のリモートアクセスシステムであって、  
前記記憶媒体に格納されたブートプログラムは、前記クライアント機器に格納された後、当該クライアント機器に備えられた記憶装置がアクセス制限がされているか否かを判断し、  
アクセス制限がされている場合、  
前記記憶媒体に格納された認証情報を用いて前記アクセス制限を解除して前記記憶装置に格納されたOSプログラムを実行することを特徴とするリモートアクセスシステム。
- [16] 請求項15記載のリモートアクセスシステムであって、  
前記ブートプログラムは、  
前記記憶媒体に格納された認証情報を用いた前記アクセス制限の解除に失敗した場合、前記記憶媒体に格納されたOSプログラムを実行することを特徴とするリモートアクセスシステム。
- [17] ネットワークを介してサーバにアクセスするクライアント機器に接続される記憶媒体

であって、

前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、業務アプリケーションと、耐タンパ格納領域に格納された前記サーバに対する遠隔操作のための認証情報と、前記クライアント機器が起動される際に該クライアント機器が有するBIOSによって実行されるブートプログラムと、OSプログラムとを有し、

前記クライアント機器のBIOSは、当該記憶媒体に格納されたブートプログラムを前記クライアント機器が有するブートプログラムよりも先に検出するように設定され、

前記クライアント機器の電源を投入後に、前記BIOSにより当該記憶媒体に格納されたブートプログラムが検出されて、当該ブートプログラムにより、当該記憶媒体に格納されたOSプログラムが前記クライアント機器に送信されることを特徴とする記憶媒体。

[18] 請求項17記載の記憶媒体であって、

前記OSプログラムを前記クライアント機器上で起動するか否かを選択するための手段を有し、

前記選択するための手段で前記OSプログラムを前記クライアント機器上で起動することを選択した場合、

前記ブートプログラムを前記クライアント機器に送信して前記OSプログラムを前記クライアント機器上で実行させ、

前記選択するための手段で前記OSプログラムを前記クライアント機器上で起動しないことを選択した場合、

ダミーデータを前記クライアント機器に送信して、前記クライアント機器に予め格納されたOSプログラムを前記クライアント機器上で実行させることを特徴とする記憶媒体。

[19] 請求項17記載の記憶媒体であって、

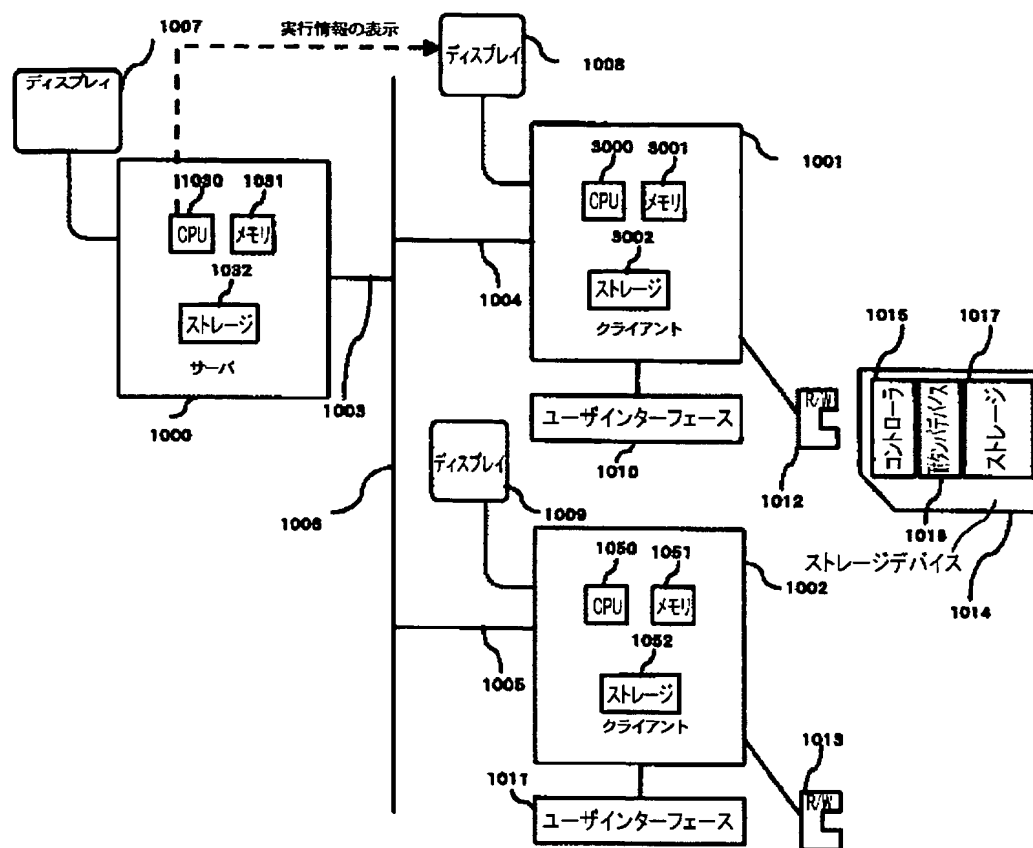
前記記憶媒体に格納されたブートプログラムは、前記クライアント機器に格納された後、当該クライアント機器に備えられた記憶装置がアクセス制限がされているか否かを判断し、

アクセス制限がされている場合、

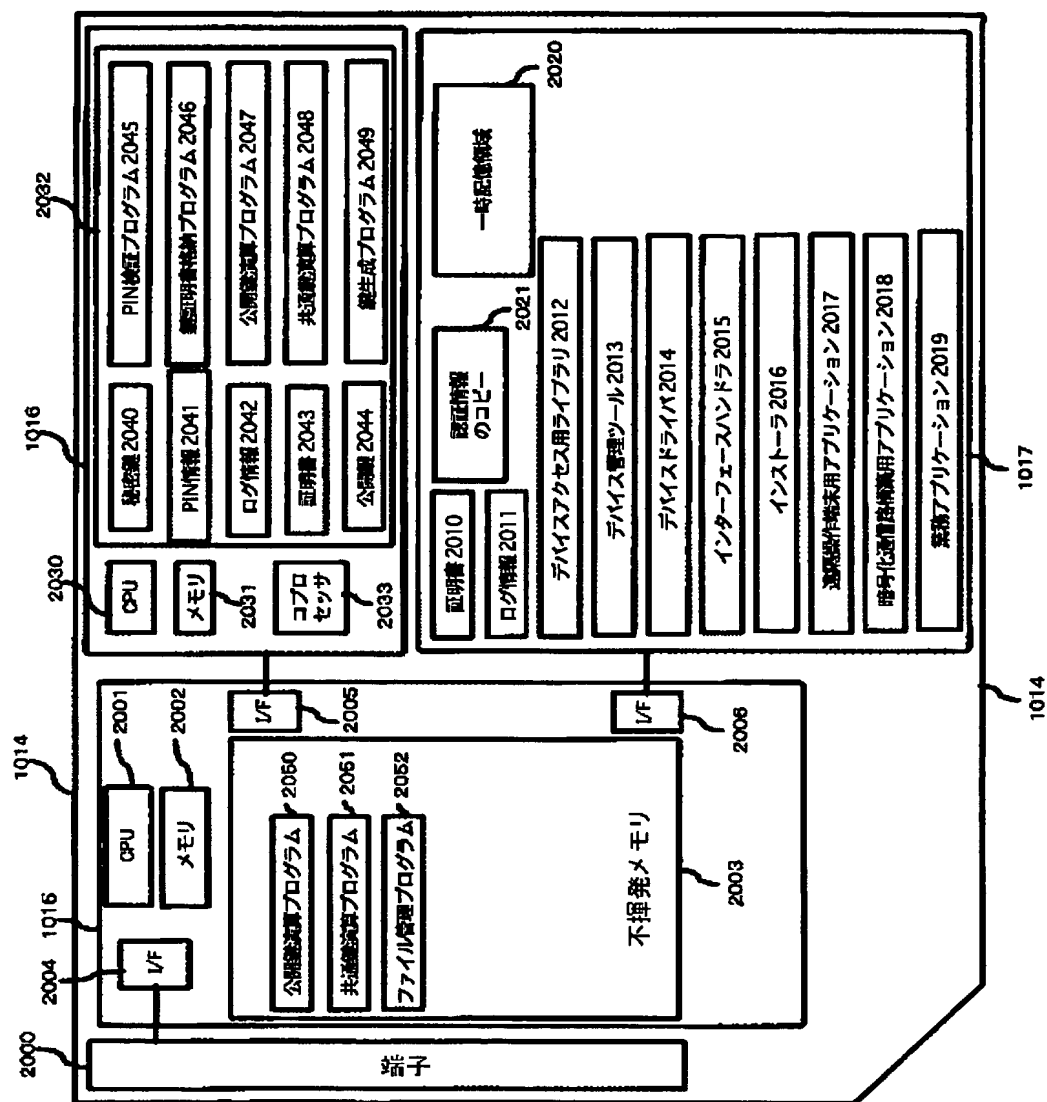
当該記憶媒体に格納された認証情報を前記クライアント機器に送信し前記アクセス制限を解除して前記記憶装置に格納されたOSプログラムを実行させることを特徴とする記憶媒体。

- [20] 請求項19記載の記憶媒体であって、  
前記ブートプログラムは、  
前記記憶媒体に格納された認証情報を用いた前記アクセス制限の解除に失敗した場合、当該記憶媒体に格納されたOSプログラムを前記クライアント機器で実行させることを特徴とする記憶媒体。
- [21] 請求項18記載の記憶媒体であって、  
当該記憶媒体は前記クライアント機器に接続されるリーダライタを有し、  
前記選択するための手段は、前記リーダライタ側に備えられることを特徴とする記憶媒体。

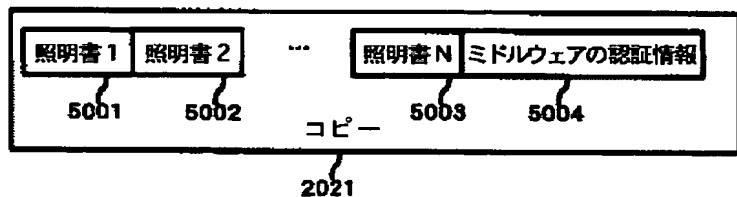
[図1]



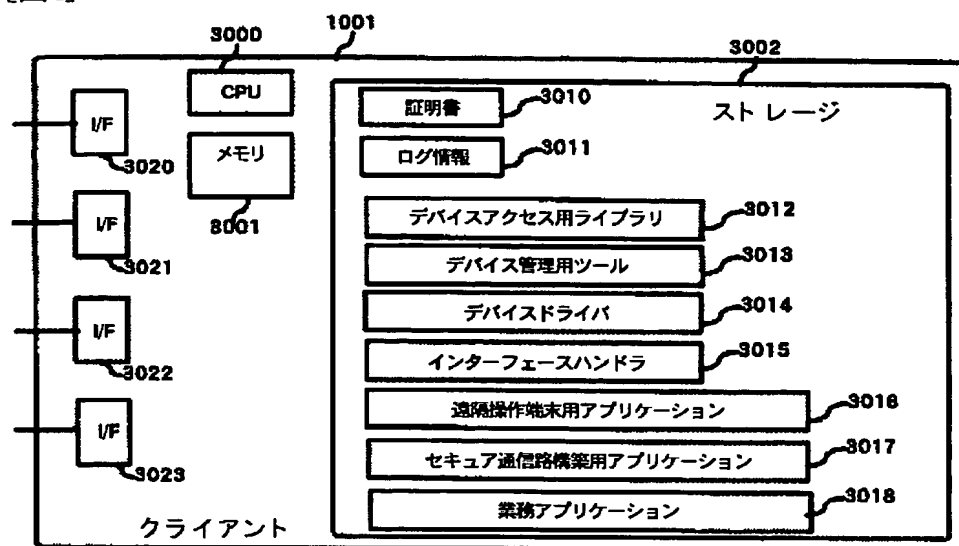
[図2]



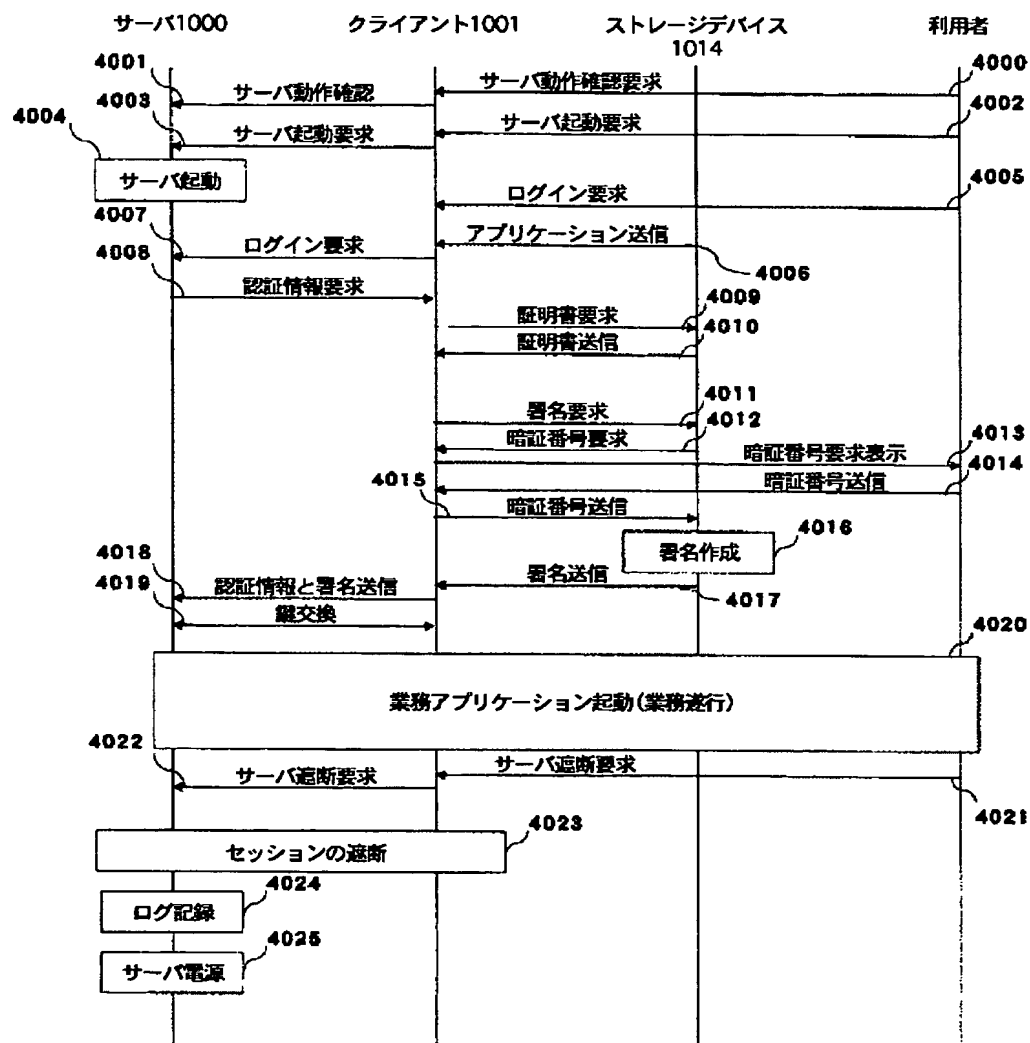
[図3]



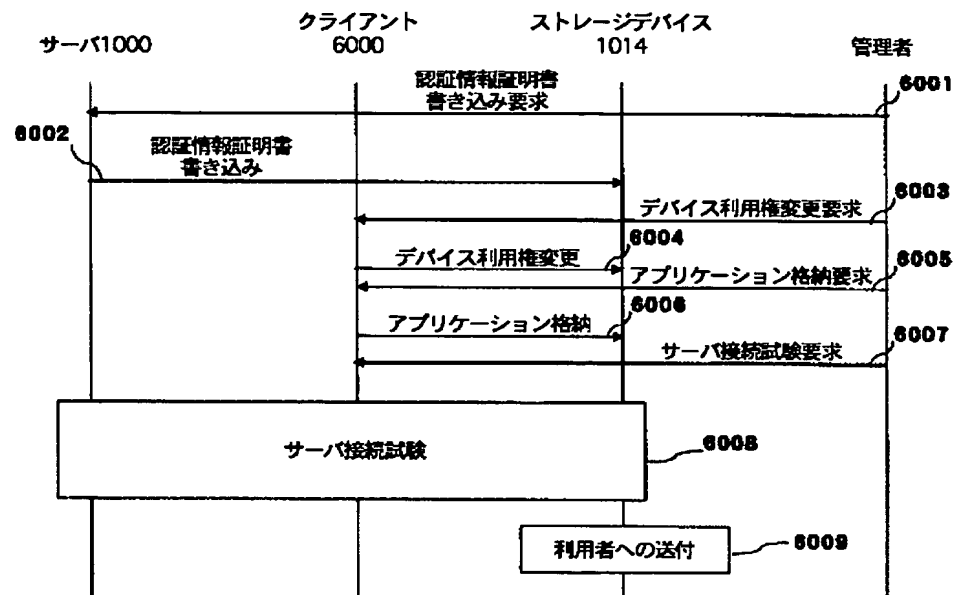
[図4]



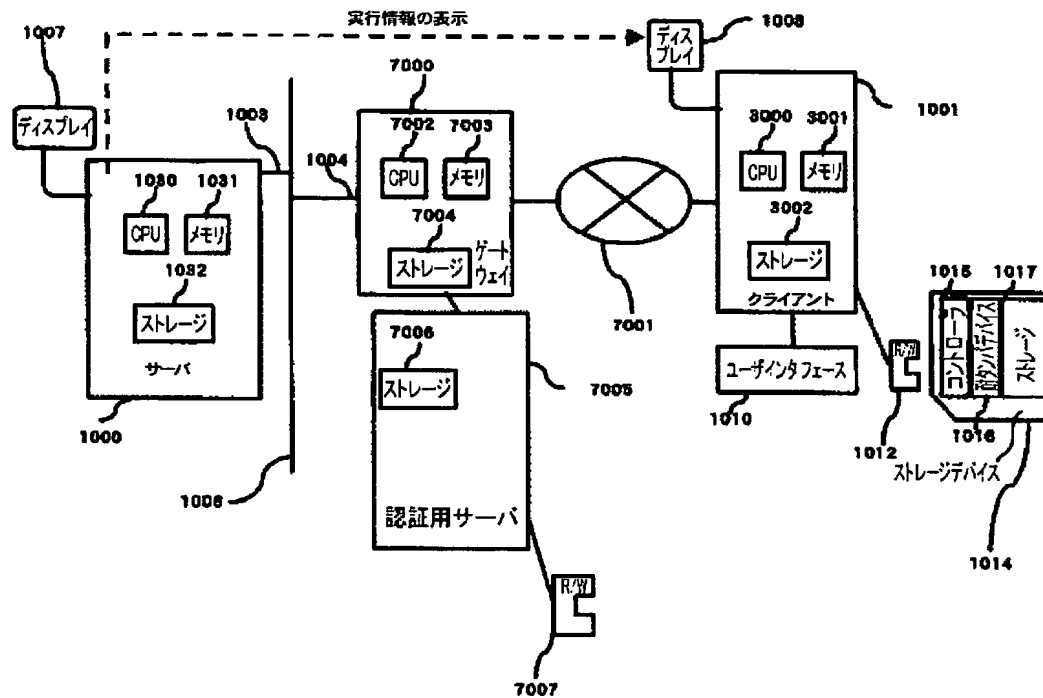
[図5]



[図6]

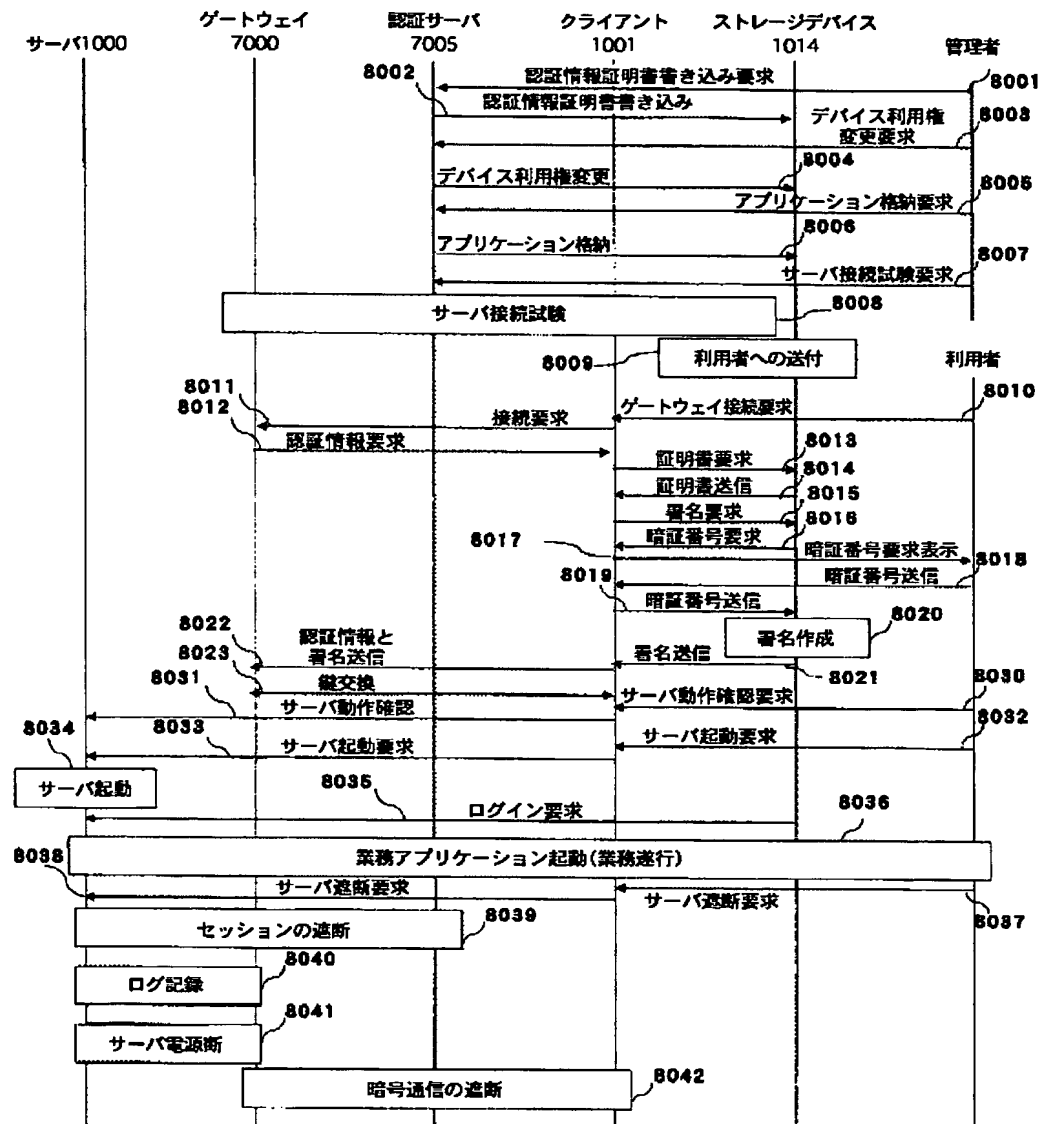


[図7]

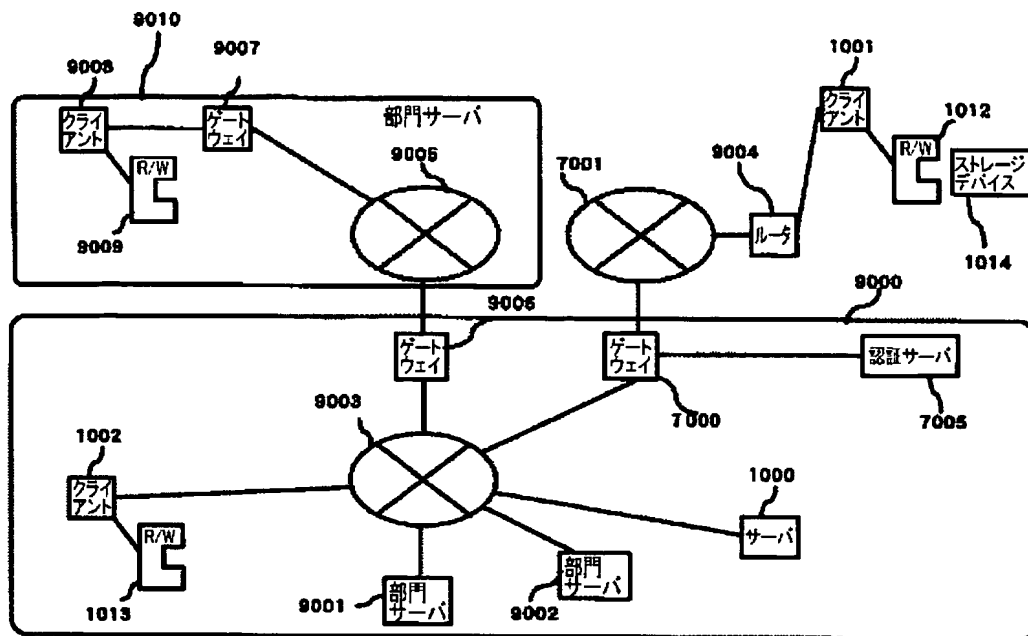




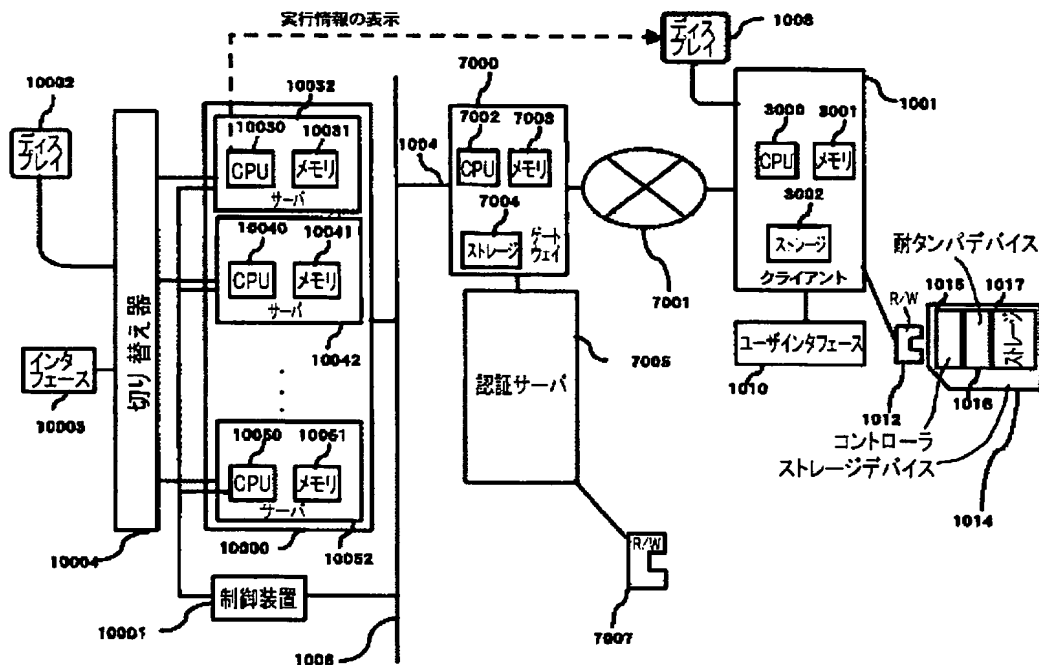
[図8]



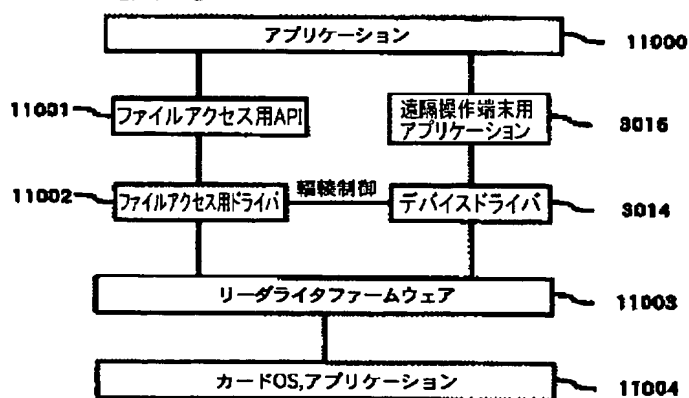
[[図9]]



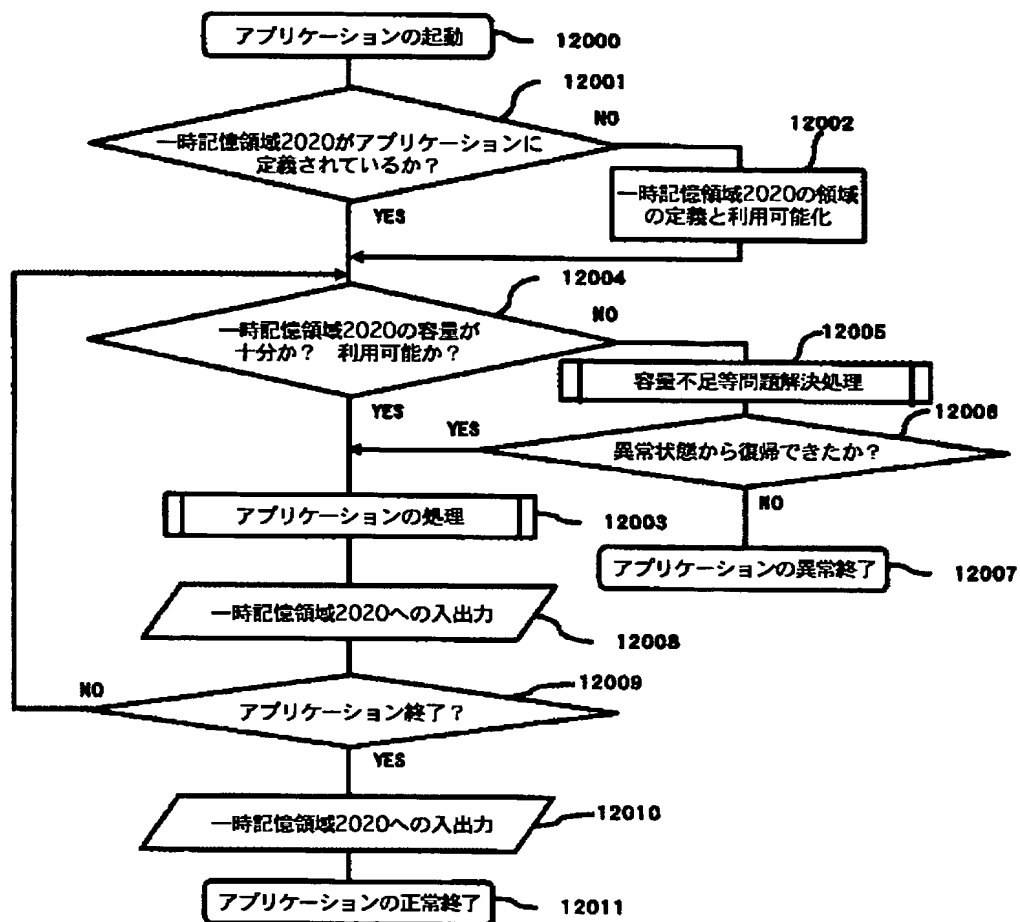
[[図10]]



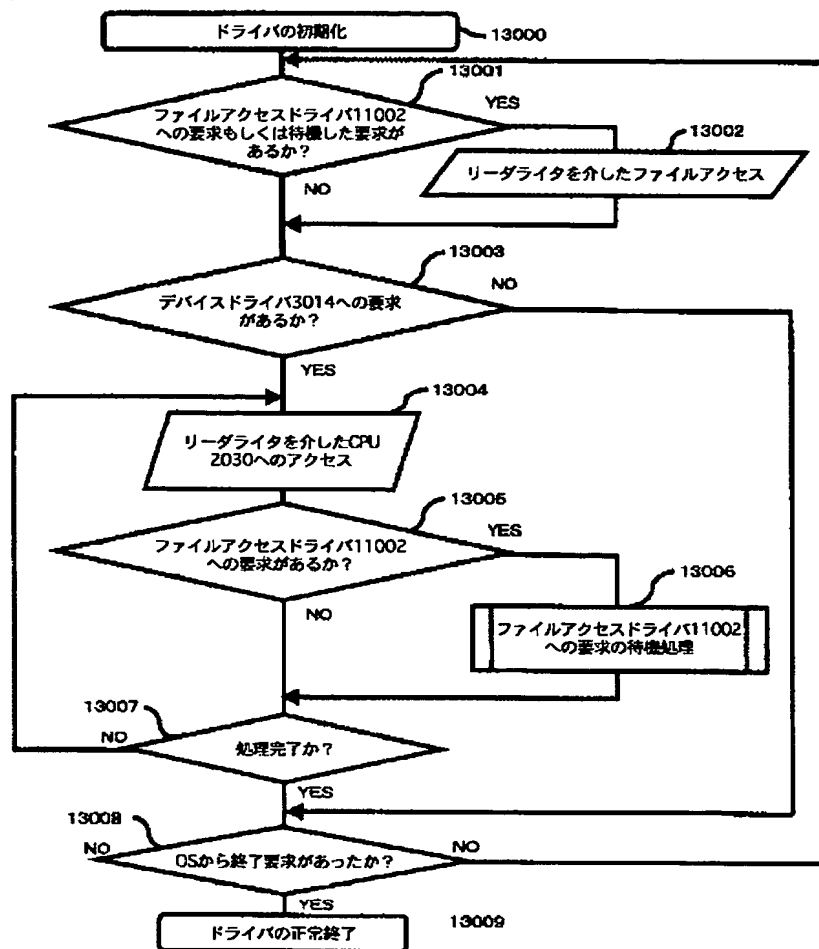
[[図11]]



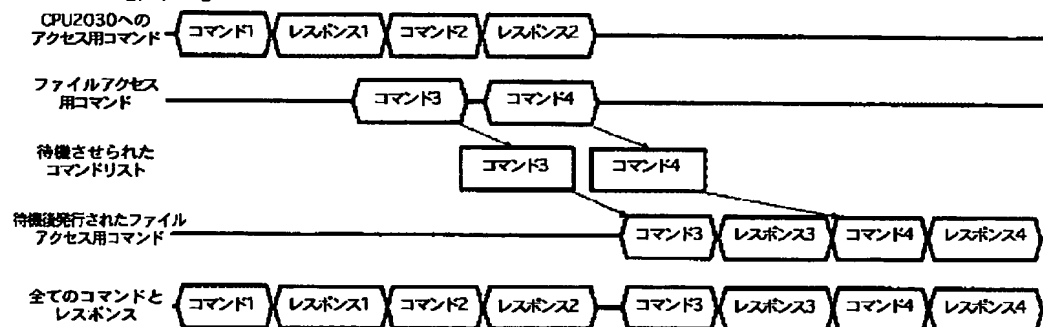
[図12]



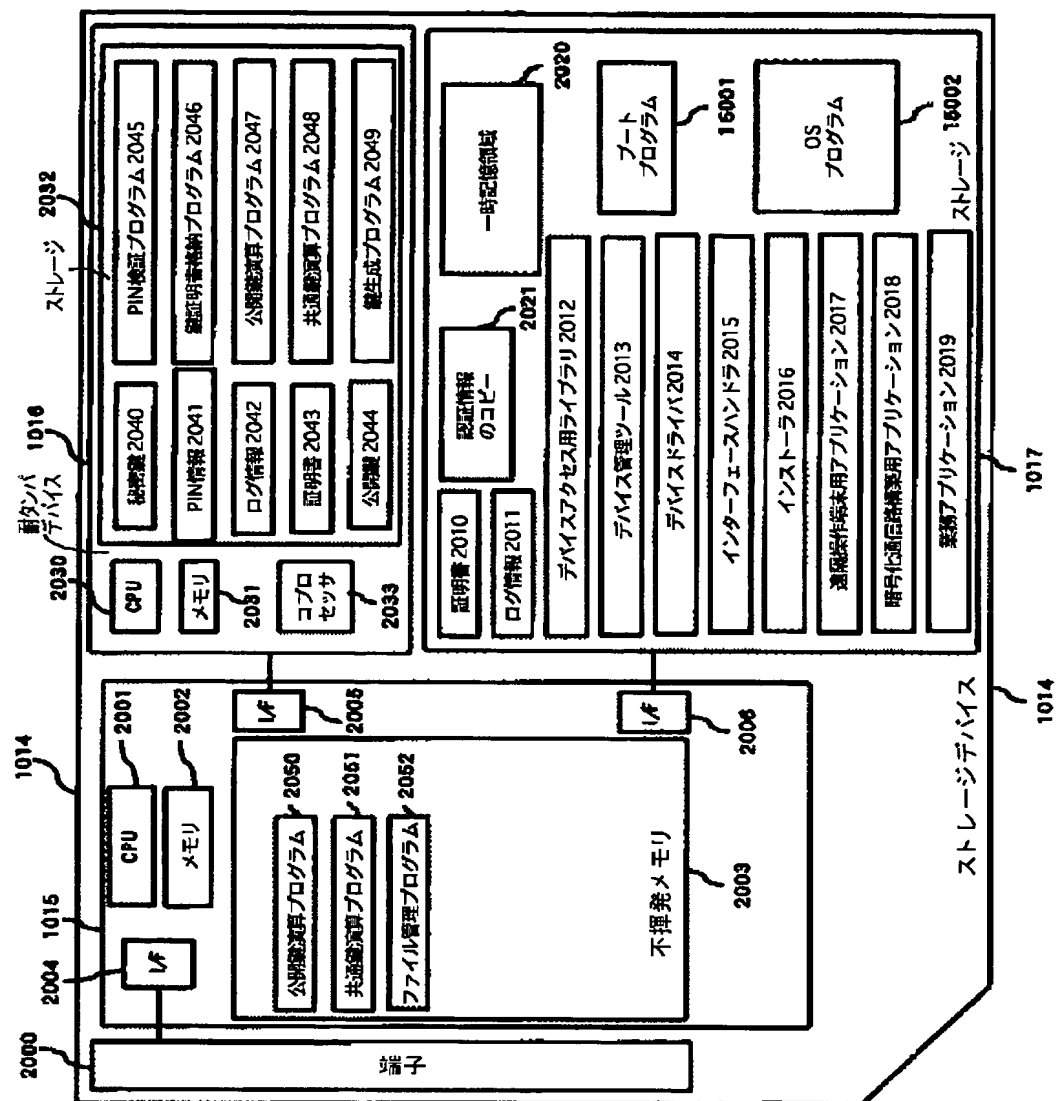
[図13]



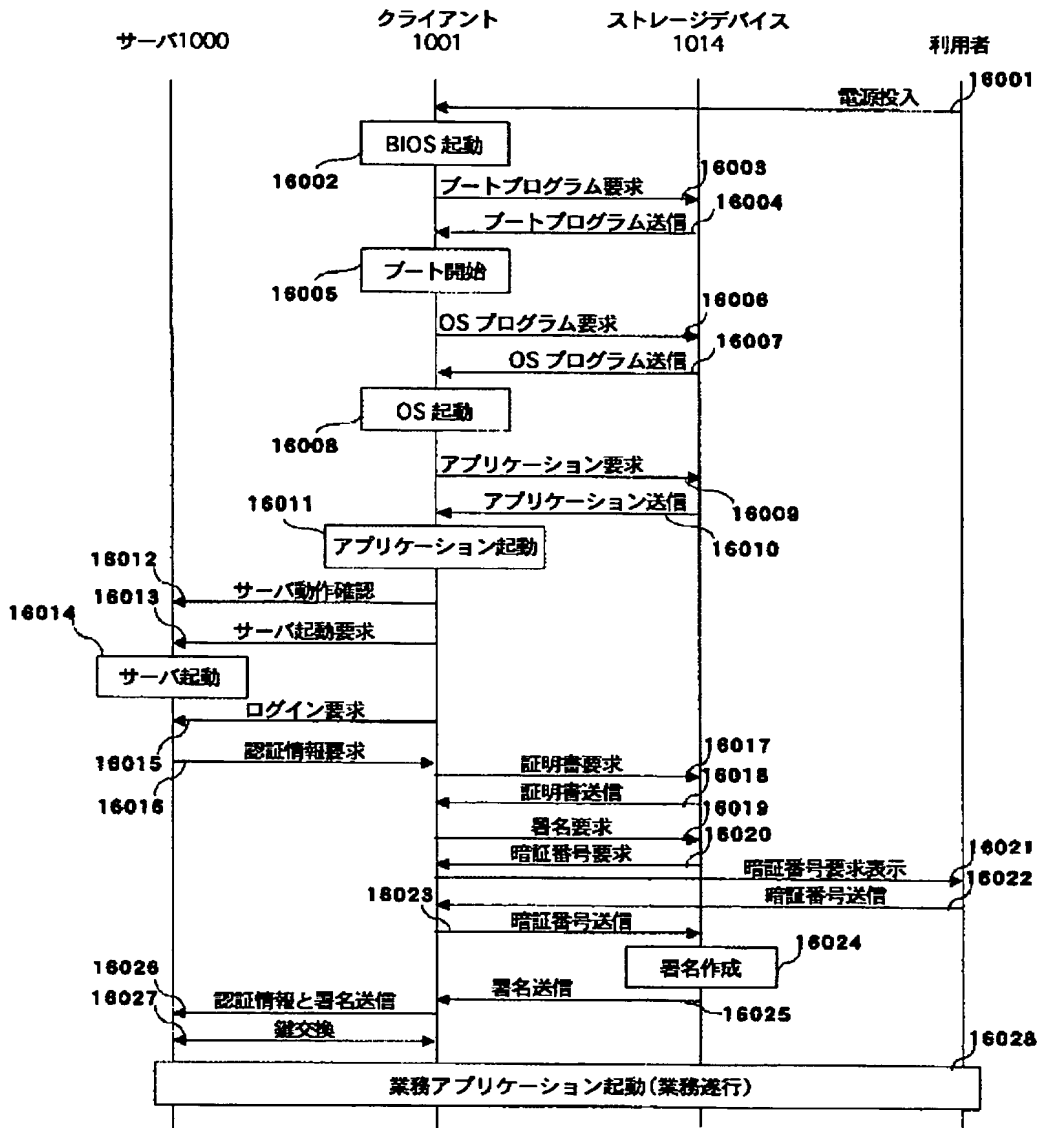
[図14]



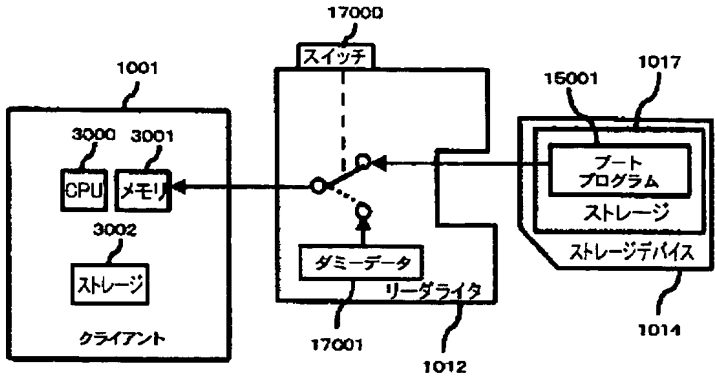
[図15]



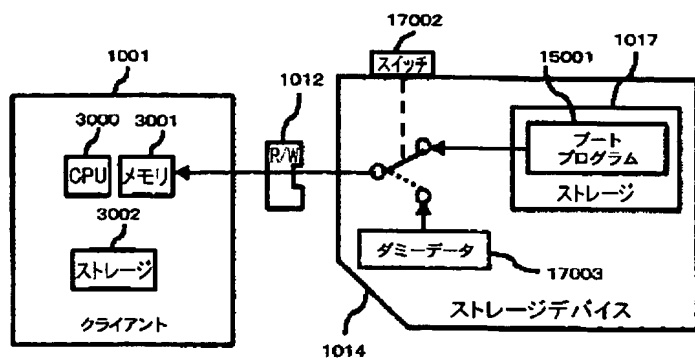
[図16]



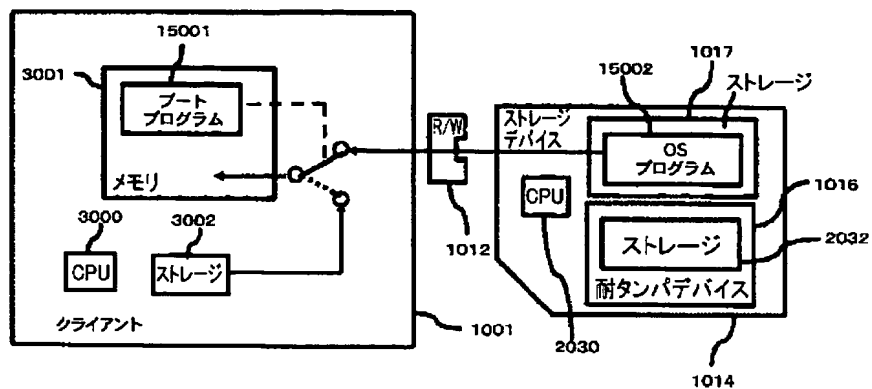
[図17A]



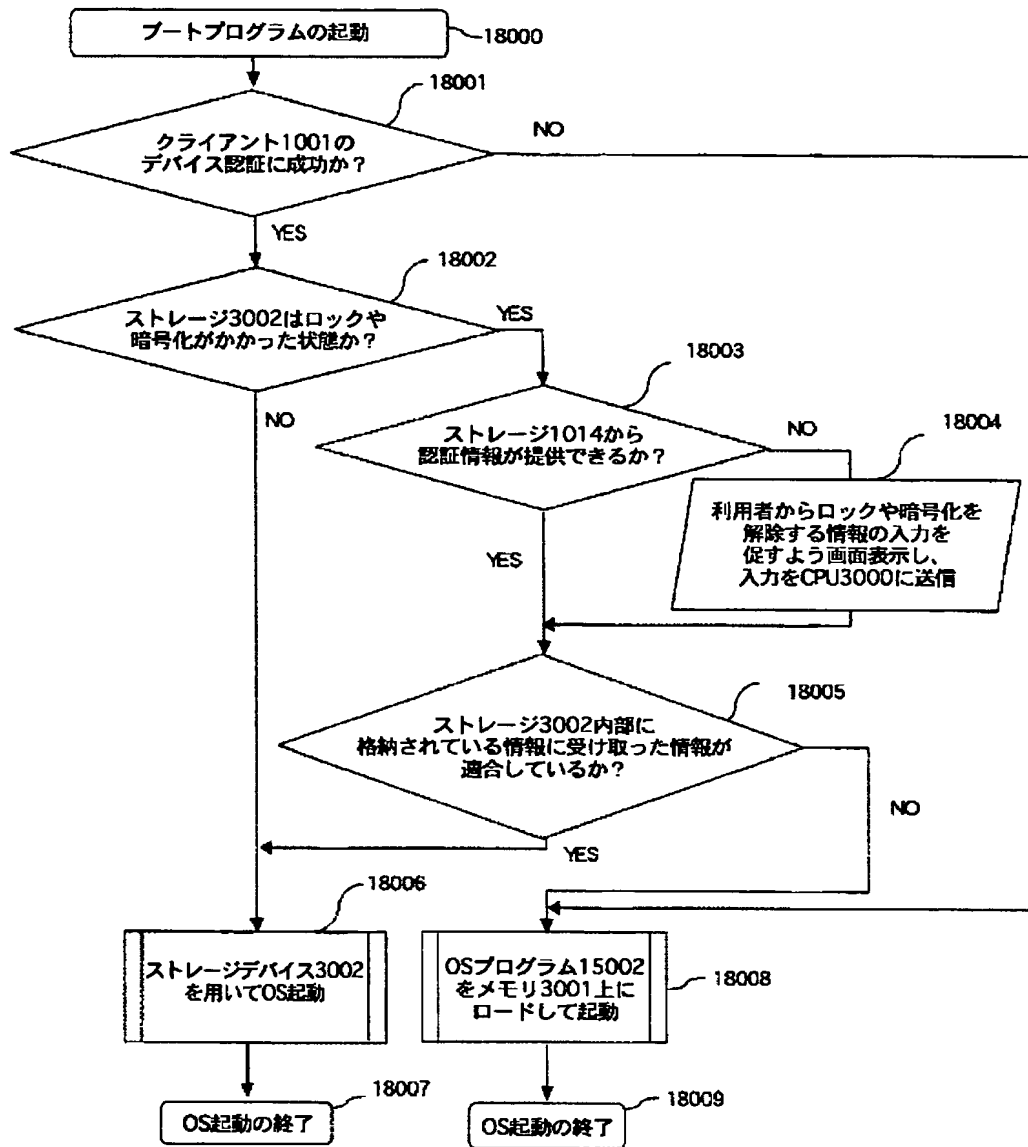
[図17B]



[図17C]



[図18]





# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/000698

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F15/00, G06F12/14, G06K17/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
CSDB (Japanese Patent Office)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MIYAKE et al., "Contents Haishin Mobile Commerce-Yo no Secure Multimedia Card", Hitachi Hyoron, Hitachi Hyoronsha, 01 October, 2001 (01.10.01), 2001 Nen 10 Gatsu special extra issue, pages 9 to 14	1-21
Y	Mitsurai Chiba, "Internet ni Okeru Personal Network no Kochiku", Information Processing Society of Japan Kenkyu Hokoku, Information Processing Society of Japan, 27 July, 2001 (27.07.01), Vol.2001, No.78, (2001-0S-88), pages 83 to 90	8
Y	JP 2003-108385 A (Toshiba Corp.), 11 April, 2003 (11.04.03), Full text; Figs. 1 to 5 (Family: none)	11-21

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier application or patent but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
23 March, 2005 (23.03.05)

Date of mailing of the international search report  
05 April, 2005 (05.04.05)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/000698

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-158650 A (Fujitsu Ltd.), 31 May, 2002 (31.05.02), Full text; Figs. 1 to 28 & US 2002-62440 A1 & EP 01209874 A	1-21
A	JP 2003-337749 A (Matsushita Electric Industrial Co., Ltd.), 28 November, 2003 (28.11.03), Full text; Figs. 1 to 7 & WO 03077083 A2 & US 2003-182569 A1	1-21

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/000698

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:  
(See extra sheet)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

- ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/000698

Continuation of Box No.III of continuation of first sheet(2)

The matter common to the inventions of claims 1-21 only relates to that a client device accesses a server via a network. Since such a client & server system is a known technique. Accordingly, the matter common to the inventions of claims 1-21 is not novel.

Furthermore, the matter common to the inventions of claims 1-9 and 11-21 relate to a storage medium including a remote operation application for operating the server at a distance, an encryption application program for encrypting the communication on network, authentication information stored in the tamper-proof storage area for remote operation of the server, and middleware. However, the search has revealed that such a storage medium is a known technique as is disclosed in the documents given below.

Document 1: Miyake et al. "Contents Haishin Mobile Commerce-Yo no Secure Multimedia Card", Hitachi Ronpyo Sha, 01 October, 2001 (01.10.01), special number of October, 2001, pp. 9-14

Document 2: JP2002-229861A (Hitachi Ltd.), 16 August, 2002 (16.08.02), whole text, all the pages (family none)

As a result, the aforementioned common matter makes no contribution over the prior art and cannot be a special technical feature within the meaning of PCT Rule 13.2, second sentence.

Accordingly, there exists no novel matter common to the inventions of claims 1-9 and 11-21.

The inventions of claims 1-9 are technically characterized in that a client device loads middleware from a storage medium and executes it, thereby performing file access and authentication. The invention of claim 10 is technically characterized in that file access and authentication are performed by operating the interface and the driver installed in the client device not having the configuration associated with the storage medium. The inventions of claims 11-21 are technically characterized in that the storage medium contains a boot program which is executed by BIOS owned by the client device and upon power ON, the client device executes the boot program in the storage medium and acquires and executes an OS program, i.e., an operation which has substantially no relation to the security is performed. Between these three groups of inventions, there exists no other common feature which can be considered as a special technical feature within the meaning of PCT Rule 13.2, second sentence. Accordingly, no technical relationship within the meaning of PCT Rule 13 between the different inventions can be seen.

Consequently, it is obvious that the inventions of claims 1-9, the invention of claim 10, and the inventions of claims 11-21 do not satisfy the requirement of unity of invention.

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl <sup>7</sup> G06F15/00		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl <sup>7</sup> G06F15/00、G06F12/14、G06K17/00、H04L9/32		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2004年 日本国実用新案登録公報 1996-2004年 日本国登録実用新案公報 1994-2004年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
CSDB (日本国特許庁)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	三宅、外2名著、"コンテンツ配信・モバイルコマース用のセキュアマルチメディアカード"、日立評論、日立評論社、2001. 10. 01、2001年10月増刊号、第9-14頁	1-21
Y	光来・千葉著、"インターネットにおけるパーソナルネットワークの構築"、情報処理学会研究報告、(社)情報処理学会、2001. 07. 27、第2001巻、第78号 (2001-OS-88)、第83-90頁	8
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	国際調査報告の発送日	
23. 03. 2005	05.04.2005	
国際調査機関の名称及びあて先	特許庁審査官 (権限のある職員)	5 B 9 1 9 3
日本国特許庁 (ISA/J P)	林 毅	
郵便番号100-8915	電話番号 03-3581-1101	内線 3546
東京都千代田区霞が関三丁目4番3号		

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2003-108385 A (株式会社東芝) 2003.04.11、全文、第1-5図 (ファミリーなし)	11-21
A	J P 2002-158650 A (富士通株式会社) 2002.05.31、全文、第1-28図 & US 2002-62440 A1 & EP 01209874 A	1-21
A	J P 2003-337749 A (松下電器産業株式会社) 2003.11.28、全文、第1-7図 & WO 03077083 A2 & US 2003-182569 A1	1-21

## 第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。  
つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

特別ページ参照。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

## (第Ⅲ欄の続き)

請求の範囲1-21に係る発明すべてに共通する事項は、クライアント機器が、ネットワークを介しサーバにアクセスすることのみであるが、このようなクライアント&サーバシステムは周知のものであるから、請求の範囲1-21に係る発明すべてに共通する事項は新規なものではない。

さらに、請求の範囲1-9及び11-21に係る発明すべてに共通する事項は、サーバを遠隔操作する遠隔操作アプリケーションと、ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、耐タンパ格納領域に格納された前記サーバに対する遠隔操作のための認証情報と、ミドルウェアを有する記憶媒体であるが、このような記憶媒体は、以下の文献に記載されているように周知であることが分かった。

文献1：三宅、外2名著、”コンテンツ配信・モバイルコマース用の  
セキュアマルチメディアカード”、日立評論、日立評論社、2001.10.01、  
2001年10月増刊号、第9-14頁

文献2：JP 2002-229861 A(株式会社日立製作所)、  
2002.08.16、全文、全頁(ファミリーなし)

その結果、上記共通の事項は、先行技術の域を出ないから、PCT規則13.2の第2文の意味において、特別な技術的特徴ではない。

したがって、請求の範囲1-9及び11-21に係る発明すべてにおいても共通の新規な事項はない。

そして、請求の範囲1-9に係る発明は、クライアント機器が記憶媒体からミドルウェアをロードして実行し、ファイルアクセス及び認証処理を行うことを技術的特徴とし、請求の範囲10に係る発明は、記憶媒体に関する構成を有しておらず、クライアント機器にインストールされたインタフェース及びドライバを動作させてファイルアクセス及び認証処理を行うことのみを技術的特徴とし、請求の範囲11-21に係る発明は、前記記憶媒体にクライアント機器が有するBIOSによって実行されるブートプログラムが格納されており、電源投入時に、クライアント機器が、記憶媒体のブートプログラムを実行しOSプログラムを取得して実行するという、実質的にセキュリティとは無関係な処理を行うことを技術的特徴としているから、3つの発明群の間には、PCT規則13.2の第2文の意味において特別な技術的特徴と考えられる共通の事項は他に存在しないので、これらの発明群の間にPCT規則13の意味における技術的な関連を見いだすことはできない。

よって、請求の範囲1-9に係る発明と、請求の範囲10に係る発明と、請求の範囲11-21に係る発明は、発明の単一性の要件を満たしていないことが明らかである。